DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

CLAUDIA BARROS QUIROZ

GIRALDO MAURY CURE

Proyecto presentado como requisito para optar el título de Magister en Gobierno de Tecnología Informática.

FUNDACION UNIVERSIDAD DEL NORTE

DIVISION DE INGENIERÍAS

MAESTRIA PROFESIONAL EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA

BARRANQUILLA – COLOMBIA

2011

TABLA DE CONTENIDO

TABLA DE FIGURAS

AGRADECIMIENTOS

Agradecemos a las personas que nos apoyaron durante nuestros estudios y que fueron grandes motivadores durante el desarrollo de este proyecto, especialmente a nuestro asesor y tutor: Ing. Jorge Alberto Gil Peñaloza.

A nuestras familias por ser nuestra fuerza, apoyo y fuente de motivación e inspiración permanente.

Gracias a Dios, por acompañarnos.

1. ANTECEDENTES

La información se ha convertido en un activo estratégico de las empresas, un activo que tiene un valor en ocasiones poco calculable hasta que se pierde y altera la trayectoria del negocio. Esta pérdida puede ser ocasionada por diferentes factores como condiciones atmosféricas extremas, actividades políticas hostiles, pérdida de los sistemas y datos informáticos, pérdida de poder, pérdida de una persona esencial, incendio, inundación o una explosión.

Según datos del Emergency Management Forum [1], el 43% de las empresas estadounidenses que afrontan un desastre sin contar con un Plan de Continuidad de Negocio nunca vuelven a la actividad, el 51% sobrevive pero tarda un promedio de dos años para reinsertarse en el mercado y sólo el 6% mantiene su negocio a largo plazo.

Actualmente, las autoridades reguladoras están insistiendo en que se adopten medidas que protejan a las organizaciones de sucesos imprevistos y a medida que los negocios evolucionan, también lo hace la dependencia a las infraestructuras de soporte. Como ejemplo sencillo, la pérdida del correo electrónico hace diez años podría haber sido una incomodidad. Hoy en día, el correo electrónico se ha convertido en un medio de comunicación fundamental para la mayoría de las organizaciones, independientemente de su tamaño, y ha sido una herramienta decisiva en el desarrollo de los mercados de alcance global.

1.1. FORMULACION DEL PROBLEMA

Un incidente no tiene que ser un dramático ataque terrorista para tener un impacto enorme en una empresa. La idea fundamental es que las empresas necesitan implementar planes que les permitan manejar incidentes, ya sean grandes ataques terroristas o pequeños problemas informáticos y, por tanto, evitar grandes interrupciones del negocio. Por esta razón, se han desarrollado directivas y estándares para la Gestión de la Continuidad del Negocio [2], que es el nombre que se da a las distintas disciplinas que tienen como objetivo promover políticas, prácticas y procesos que estén al servicio de las medidas de protección que hoy en día existen en los mercados financieros y que deben ser adoptadas por las organizaciones. Algunos de estos estándares son ***British Standard - 25999*** [3] para la Gestión de la Continuidad del Negocio, el proceso de "Gestión de la continuidad de los servicios IT" en la etapa de "Diseño del servicio" de ***ITIL*** [4] o el proceso "DS4 - Asegurar la continuidad del servicio" del domino "Entrega y soporte" del estándar ***COBIT*** [5].

Para las grandes organizaciones, la gestión de la continuidad del negocio se lleva a cabo durante todo el tiempo, por una persona o un pequeño equipo (de acuerdo al tamaño del negocio). Pero para la gran mayoría de las empresas, esta función será probablemente la responsabilidad de una persona que haga este trabajo además de sus funciones diarias, o algunas ni siquiera tienen contemplado un plan de continuidad, debido a la falta de formación y de información sencilla, detallada y que ilustre las fases, tareas y actividades para confeccionar un Plan de continuidad ágilmente.

2. JUSTIFICACION

En la actualidad, la creciente competitividad entre las organizaciones, las demandas de los clientes cada vez más exigentes o los requerimientos normativos rigurosos son factores que obligan a las empresas a adoptar nuevas estrategias a fin de garantizar el éxito y demostrar la resistencia de las operaciones de negocio ante cualquier eventualidad grave. Sin embargo, acorde con la experiencia de los autores de este escrito y la literatura existente en la materia, el nivel de implantación de planes de continuidad de negocio en las pequeñas y medianas empresas es notablemente inferior si se compara con las grandes empresas quienes disponen de los recursos técnicos, económicos y humanos necesarios para convertir esta necesidad en una realidad.

Si bien existen multitud de manuales, estándares y recomendaciones que tratan de guiar a las organizaciones a adoptar estrategias de continuidad de negocio, la mayoría de ellas son teóricas, expresadas con un lenguaje formal, y no tienen en cuenta la situación, problemática, necesidades reales o niveles de conocimiento de las organizaciones.

Este proyecto de carácter académico, busca disminuir estos niveles de desorientación, a través de un marco de metodológico de actuación para aquellas organizaciones (sin importar el sector, actividad, ubicación geográfica, ni tamaño) que deseen entender y abordar los principios y las prácticas de continuidad de negocio desde el momento en que se reconoce la necesidad de desarrollar un a estrategia de continuidad, hasta su mantenimiento y actualización constante.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Diseñar un marco metodológico para el desarrollo de un Plan de Continuidad del Negocio en una compañía, soportado en estándares de Gestión de la Continuidad del Negocio.

3.2. OBJETIVOS ESPECIFICOS

Explorar e interpretar el estándar BS 25999, el proceso Gestión de la Continuidad de los Servicios de TI de ITIL y el proceso "DS4 - Asegurar la continuidad del servicio" del dominio "Entrega y soporte" de COBIT. A partir de dicha exploración

- Diseñar un Marco Metodológico para desarrollar un Plan de Continuidad del Negocio adaptable a cualquier empresa.
- Desarrollar una guía de implantación de dicho marco, donde se muestren cada una de las fases que componen un Plan de Continuidad del negocio.
- Describir las actividades a desarrollar en cada una de las fases del Plan de Continuidad del Negocio.
- Seleccionar los procesos claves para la efectiva Gestión de la Continuidad y preparar los procedimientos requeridos para cada proceso.

4. MARCO TEORICO

4.1. DEFINICIONES

AMENAZA: eventos que, aprovechando una vulnerabilidad, pueden desencadenar un incidente en la empresa, produciendo daños materiales o pérdidas inmateriales en sus activos. Dentro de eventos se consideran tanto acciones, como interrupciones o falta de acción.

DESASTRE: problema o evento no planificado, caya consecuencia es la interrupción de los procesos de negocio durante un periodo de tiempo. Este tiempo de paralización de los procesos es superior a lo que la organización puede soportar sin sufrir perjuicios considerables para el negocio.

GOBIERNO DE TI: Consiste en un completo marco de estructuras, procesos y mecanismos relacionales. Las estructuras implican la existencia de funciones de responsabilidad, como los ejecutivos y responsables de las cuentas de TI, así como diversos comités de TI. Los procesos se refieren a la monitorización y a la toma de decisiones estratégicas de TI. Los mecanismos relacionales incluyen las alianzas y la participación de la empresa/organización de TI, el dialogo en la estrategia y el aprendizaje compartido. [6]

GESTION DE LA CONTINUIDAD: es un proceso integral que identifica los impactos potenciales que amenazan una organización y proporciona un marco para la construcción de la resiliencia y la capacidad para dar una respuesta eficaz

que salvaguarde los intereses de sus principales partes interesadas, la reputación, la marca y el valor de la creación de actividades.

IMPACTO: consecuencia evaluada de una interrupción.

INCIDENTE: cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar una interrupción o una reducción de la calidad de ese servicio.

INTERDEPENDENCIAS: relaciones establecidas entre el conjunto de equipamiento, personas, tareas, departamentos, mecanismos de comunicación y proveedores externos que constituye una actividad de negocio.

INTERRUPCIÓN: suspensión de las operaciones normales del negocio durante un período de tiempo.

PLAN DE CONTINUIDAD DE NEGOCIO (PCN) o BUSINESS CONTINUITY PLAN (BCP por sus siglas en inglés) es un conjunto de directrices, criterios, normas de actuación y herramientas organizativas que, ante la ocurrencia de una contingencia que provocase la interrupción de alguna o todas las áreas de negocio de una organización, permitan la recuperación de la operatividad de las mismas en el menor tiempo posible, de modo que las pérdidas económicas ocasionadas sean mínimas.

RESILIENCIA: término de origen inglés (resilient) referido a la capacidad de elasticidad y resistencia de una empresa para hacer frente a los impactos.

RIESGO: probabilidad de que una amenaza aproveche y explote una debilidad asociada a un proceso/activo/recurso provocando daño sobre el mismo.

TELETRABAJO: desempeño de un trabajo de manera regular en un lugar diferente del centro de trabajo habitual, generalmente empleando medios informáticos.

VULNERABILIDAD: debilidad o falta de control asociada a un proceso o recurso que puede ser explotada provocando un daño sobre dicho proceso.

4.2. GENERALIDADES [7]

La Gestión de Continuidad de Negocio es un proceso integral de gestión que identifica los posibles impactos que amenazan a una organización y ofrece un marco para proporcionar robustez y disponer de una respuesta efectiva que salvaguarde los intereses de los principales proveedores, clientes y demás partes interesadas, la reputación, la marca y las actividades creadoras de valor.

La GCN tiene que ser asimilada y totalmente integrada en la organización como uno más entre sus procesos de gestión.

La GCN aspira a mejorar la capacidad de recuperación de una organización. Al identificar por adelantado los posibles impactos de una amplia gama de incidencias que trastornarían de forma súbita el éxito de la organización, establece prioridades para los esfuerzos de los especialistas en implantar robustez en sus respectivas áreas de especialización, como seguridad, instalaciones y tecnologías de la información.

Si bien se interesa por todo tipo de mecanismos de fortaleza o robustez, la GCN se centra particularmente en desarrollar una capacidad de recuperación que sea conjunta para toda la organización y le permita sobrevivir a la pérdida total o parcial de su capacidad operativa. También debería enfocarse en soportar pérdidas significativas de recursos, como personal o maquinaria.

Debido a que la capacidad de resistencia de la GCN de una organización depende de su equipo de gestión y su personal, además de su tecnología y la diversificación geográfica, se debe desarrollar esta capacidad de recuperación a todos los niveles de la organización, desde la alta dirección hasta el taller, y en todos los demás integrantes de la cadena de valor.

El factor determinante de esta robustez en toda la organización se sustenta en la responsabilidad de la alta dirección de proteger los intereses a largo plazo del personal, clientes y todos aquellos que dependen de algún modo de la organización. Si bien se pueden calcular las pérdidas financieras ocasionadas por una interrupción, generalmente el mayor daño suele reflejarse en una pérdida de imagen o de confianza fruto de un incidente mal gestionado. Del mismo modo, un incidente bien gestionado puede mejorar la imagen de la organización y su equipo de gestión.

La base de la gestión de la continuidad son las políticas, guías, estándar y procedimientos implementados por una organización. Todo el diseño, implementación, soporte y mantenimiento de los sistemas debe estar fundamentado en la obtención de un buen plan de continuidad del negocio, recuperación de desastres y en algunos casos, soporte al sistema. En ocasiones la gestión de la continuidad se confunde con la gestión de la recuperación tras un desastre, pero son conceptos diferentes. La recuperación de desastres es una pequeña parte de la gestión de la continuidad.

Los objetivos principales de la Gestión de la Continuidad se resumen en: garantizar la pronta recuperación de los servicios (críticos) tras un desastre, establecer políticas y procedimientos que eviten, en la medida de lo posible, las consecuencias de un desastre o causa de fuerza mayor.

Los principales beneficios de una correcta Gestión de la Continuidad se resumen en: se gestionan adecuadamente los riesgos, se reduce el periodo de interrupción

del servicio por causas de fuerza mayor, se mejora la confianza en la calidad del servicio entre clientes y usuarios.

Las principales dificultades a la hora de implementar la Gestión de la Continuidad se resumen en: puede haber resistencia a realizar inversiones cuya rentabilidad no es inmediata, no se presupuestan correctamente los costos asociados, no se asignan los recursos suficientes, no existe el compromiso suficiente con el proceso dentro de la organización y las tareas y actividades correspondientes se demoran perpetuamente para hacer frente a "actividades más urgentes", no se realiza un correcto análisis de riesgos y se obvian amenazas y vulnerabilidades reales, el personal no está familiarizado con las acciones y procedimientos a tomar en caso de interrupción grave de los servicios.

La Gestión de la Continuidad está destinada al fracaso sino se destina una cantidad de recursos suficientes, tanto en el plano humano como de equipos. Su dimensión depende de su alcance y sería absurdo instaurar una política demasiado ambiciosa que no cuente con los recursos correspondientes.

En la actualidad casi todas las empresas, grandes y pequeñas, dependen en mayor o menor medida de los servicios informáticos, por lo que cabe esperar que una interrupción de los servicios TI afecte a prácticamente todos los aspectos del negocio. Sin embargo, es evidente que hay servicios TI estratégicos de cuya continuidad puede depender la supervivencia del negocio y otros que simplemente aumentan la productividad de la fuerza comercial y de trabajo.

El objetivo de la Gestión de la Continuidad de TI es apoyar los procesos empresariales, asegurando que las instalaciones técnicas y de servicio de TI (incluyendo sistemas informáticos, redes, aplicaciones, repositorios de datos, telecomunicaciones, medio ambiente, apoyo técnico y mesa de servicios) se

puedan reanudar, según los plazos de tiempo acordados. Los servicios TI no son sino una parte, aunque a menudo muy importante, del negocio.

Es importante diferenciar entre desastres como incendios, inundaciones, etc., y desastres "puramente informáticos", tales como los producidos por ataques distribuidos de denegación de servicio o virus informáticos. Aunque es responsabilidad de la ITSCM prever los riesgos asociados en ambos casos y restaurar el servicio TI con prontitud, es evidente que recae sobre la ITSCM una responsabilidad especial en el último caso pues: sólo afectan directamente a los servicios TI pero paralizan a toda la organización, son más previsibles y más habituales, la percepción del cliente es diferente los desastres naturales son más asumibles y no se asocian a actitudes negligentes, aunque esto no sea siempre cierto.

4.3. ESTANDAR BS-25999

El BS-25999 es un estándar británico que establece mejores prácticas, recomendaciones y actividades específicas para lograr la continuidad de negocio teniendo en cuenta los riesgos a los que se enfrenta una organización. Este estándar se basa en el Plan de Continuidad del Negocio o BCP por sus siglas en inglés (Business Continuity Planning) el cual, al ser implementado en una organización, se le debe hacer un seguimiento con el fin de conocer su evolución permanente en los procesos de la empresa. El BS-25999 posee dos partes esenciales: Desarrollo del BCM e Implementación del mismo.

CICLO DE VIDA DE LA GESTION DE LA CONTINUIDAD DEL NEGOCIO [8]

Figura 1. Ciclo de Vida de la Gestión de la ContinuidadDelNegocio

Fuente. BS-25999-1

ETAPA 1 – COMPRENDER LA ORGANIZACIÓN

Busca identificar los productos y servicios clave de una organización, y tras ello definir los factores críticos de las actividades que están detrás. Esta parte de la GCN debe estar totalmente integrada dentro de los objetivos, obligaciones y estatutos de la organización. Las herramientas para comprender su negocio desde un punto de vista de continuidad de negocio son:

Análisis del Impacto en el Negocio.

Un proceso obligatorio para calcular el impacto en el tiempo de una interrupción en la capacidad de operar de una organización. Identifica la urgencia de cada actividad de negocio llevada a cabo por la organización al evaluar el impacto en el tiempo de una interrupción de esta actividad en la entrega de productos y servicios. Se utiliza esta información para identificar el plazo de las estrategias de continuidad y recuperación apropiadas para cada actividad por separado y entre ellas.

Algunos métodos, herramientas y técnicas para llevar a cabo los Análisis de Impacto en el Negocio son: talleres, cuestionario (s) - en papel y/o software, entrevistas (estructuradas y no estructuradas).

Los resultados de un Análisis del Impacto en el Negocio son:

- El Período Máximo Tolerable de Interrupción y su justificación (naturaleza de los impactos) para cada actividad
- El Objetivo de Punto de Recuperación (OPR) al que la información tiene ser restaurada para permitir que una actividad opere una vez que se ha reiniciado.

Un Análisis del Impacto en el Negocio debería revisarse como mínimo una vez al año, pero de forma más frecuente en caso de: un cambio importante en el negocio

a un ritmo particularmente agresivo, un cambio importante en los procesos internos de negocio, ubicación o tecnología, un cambio importante en el entorno externo de negocio, como un cambio en el mercado o en las leyes.

Análisis de Requisitos de Continuidad.

Para calcular los recursos, instalaciones y servicios que necesitará cada actividad cuando se reinicia. Ofrece la información que permitirá determinar la magnitud (tamaño y cantidad) de las medidas apropiadas de continuidad.

Los métodos, herramientas y técnicas para llevar a cabo un Análisis de Requisitos de Continuidad incluyen talleres, cuestionario (s) - en papel y/o software, entrevistas estructuradas o no estructuradas, ee suele recoger esta información al mismo tiempo que la información relativa al AIN.

Los resultados de un Análisis de Requisitos de Continuidad son

- Los recursos que se necesitan durante el tiempo después del retorno de la actividad para ofrecer los niveles de servicio acordados.
- Las interdependencias entre actividades internas y proveedores externos.

Esta información alimenta de forma directa la etapa de creación de una Estrategia de Continuidad de Negocio. Las necesidades de recursos ofrecerán los datos para evaluar soluciones alternativas de recuperación que se adecuen en tamaño y resultados.

La revisión del análisis de requisitos de continuidad debería realizarse al mismo tiempo que la del AIN.

Evaluación de Riesgos.

Para calcular la probabilidad de amenazas conocidas y su impacto sobre funciones específicas. Ayuda a identificar las posibles causas de interrupción en una organización, la probabilidad de que suceda y el impacto en caso de que la amenaza se materialice. A partir de entonces se pueden detectar medidas que reduzcan la probabilidad de que suceda o aminoren el impacto de un incidente que se produzca por estas amenazas.

Los métodos, herramientas y técnicas para llevar a cabo una Evaluación de Riesgos son: Análisis del Árbol de Eventos, Análisis del Árbol de Fallos, Matriz de Vulnerabilidad a las Amenazas, Matriz de Riesgo, Análisis de coste y beneficio.

Los resultados de una Evaluación de Riesgos deben identificar y documentar:

- Los puntos específicos de fallo.
- Una lista de amenazas a la organización o a los procesos de negocio analizados, clasificadas por orden prioritario.
- Información para una estrategia de gestión de control de riesgos y un plan de acción para atajar los riesgos
- Aceptación demostrada de los riesgos identificados que no se van a atajar.

Se debe realizar la Evaluación de Riesgos tal y como está definida en la estrategia de gestión de riesgos de la organización. Normalmente tendrá una periodicidad anual para aquellos procesos más sensibles a los tiempos, pero será más frecuente si: El ritmo en la evolución del negocio es particularmente agresivo. Se han producido importantes cambios en el negocio en lo que se refiere a los procesos internos, la ubicación o los recursos tecnológicos, Se ha registrado una modificación importante en el entorno del negocio, Ej. un cambio en el mercado o en las obligaciones legales.

ETAPA 2 – DETERMINAR LA ESTRATEGIA DE CONTINUIDAD DE NEGOCIO

Su objetivo es poner en marcha medidas que reduzcan la probabilidad de que sucedan incidentes o aminorar su impacto en caso de que sucedan. En la etapa anterior se averiguó el Período Máximo Permitido (MTD) de Interrupción para cada producto y servicio dentro del alcance del programa. Al entender sus interdependencias se habrá podido determinar el MTD para cada actividad. En la etapa de Estrategia se debe fijar el Tiempo Objetivo Recuperación (RTO) para cada actividad dentro del MTD.

El RTO es el principal indicador de las tácticas de continuidad del lugar de trabajo adecuadas.

- Un RTO de varios meses puede permitir a la organización esperar a tomar decisiones hasta después del incidente.
- Un RTO de más de un día o dos puede permitir tiempo para la reubicación del personal a otro emplazamiento
- Un RTO de menos de un día obligará a asumir tácticas que permitan que el personal en otra ubicación se haga cargo de la actividad - lo que significa que la otra ubicación tendrá disponibilidad inmediata de los recursos necesarios para esa actividad, además de información actualizada Una vez que se ha definido el RTO, el coste y la disponibilidad determinarán la elección de las tácticas.

Los resultados de esta etapa incluyen: una estrategia para cada producto y servicio bajo el programa de GCN y una selección de las alternativas adecuadas para cada actividad, un plan para la puesta en marcha de la estrategia acordada, un conjunto de recursos y servicios de recuperación que pueden desplegarse bajo el auspicio del Plan de Continuidad de Negocio (PCN) y que permite la restauración de un nivel de funcionamiento aceptable para las actividades de

negocio dentro de su Tiempo de Recuperación (RTO) y con información recuperada de sus Objetivos de Punto de Recuperación (RPO).

Al menos cada 12 meses se debería realizar una revisión de la estrategia de GCN para cada producto y servicio. No obstante, ciertos acontecimientos pueden causar una reevaluación de la estrategia, como: una revisión del Análisis del Impacto en el Negocio que detecte cambios substanciales en los procesos y prioridades, un cambio importante en la actitud frente al riesgo de la organización, condiciones de mercado, adquisición o fusión, nuevos productos o servicios, obligaciones legales, cambios en los requisitos para la recuperación de una actividad, un cambio importante en la asignación, personal o tecnología disponible que pueda ofrecer nuevas estrategias de recuperación o un cambio en la disponibilidad de los servicios de recuperación en las inmediaciones de la organización. Puede tratarse de un cierre, fusión o apertura de una instalación.

ETAPA 3 – DESARROLLAR Y PONER EN PRÁCTICA LA GESTION DE LA CONTINUIDAD DE NEGOCIO

Abarca el desarrollo de planes de acción detallados para garantizar la continuidad de las actividades y una gestión efectiva de incidentes. El objetivo de los diversos planes abordados en esta etapa es identificar tanto como sea posible las acciones y recursos necesarios para permitir que la organización gestione una interrupción de cualquier naturaleza.

Los requisitos clave para una respuesta efectiva son:

- Un procedimiento claro para la escalada y control de un incidente
- Comunicación con proveedores, clientes y demás partes interesadas
- Planes para reiniciar las actividades interrumpidas

Se puede llegar a esto por varios medios, y aquí sólo se describe una posible estructura. Pero al margen de la estructura que se adopte, es importante que la estrategia esté de acuerdo con la cultura de la organización. Como todos los incidentes son diferentes, las acciones descritas en los planes no pretenden cubrir cada una de las eventualidades. Cualquier procedimiento predefinido puede necesitar ser adaptado con flexibilidad e iniciativa por los responsables de poner en marcha el plan al incidente específico que haya ocurrido y las oportunidades que haya creado.

Plan de Gestión de Incidentes

El propósito de un PGI es ofrecer un marco de acción que permita a una organización gestionar cualquier crisis sin importar la causa (incluyendo aquellas en la que no existe una respuesta de Continuidad de Negocio adecuada, como en el caso de una amenaza a la reputación).

Plan de Continuidad del Negocio

El propósito de un Plan de Continuidad de Negocio es ofrecer un marco de acción y procesos documentados para que la organización pueda reiniciar todos sus procesos de negocio dentro de sus Objetivos de Tiempos de Recuperación. Un Plan de Continuidad de Negocio en sí mismo no demuestra que se posea capacidades para la GCN, pero el hecho de que exista un plan actualizado en la organización sugiere que existe una capacidad efectiva.

Los pasos clave en el desarrollo de un Plan de Continuidad de Negocio (PCN) son:

- Nombrar a un responsable del Plan de Continuidad de Negocio (o de cada plan para varias ubicaciones)

- Definir los objetivos y alcance del plan en referencia a la estrategia de la organización y la Política de GCN
- Desarrollar y aprobar un proceso de planificación y un programa
- Crear un equipo de planificación para llevar a cabo el desarrollo del plan
- Decidir la estructura, formato, componentes y contenido del plan
- Determinar las estrategias que describirá el plan y qué es lo que se abordará en otros planes
- Determinar las circunstancias que superan el alcance del PCN
- Recopilar información para elaborar el plan
- Hacer un borrador del plan
- Circular el borrador del plan para consultas y revisiones
- Obtener las reacciones a las consultas
- Corregir el plan en lo que se considere adecuado
- Acordar un programa constante de pruebas y mantenimiento para garantizar que está actualizado
- Probar el plan mediante un ensayo sobre el papel

Planes de Respuesta por Actividad

El propósito del Plan Operativo de Respuesta es estructurar la respuesta de cada departamento a una interrupción dentro del Plan de Continuidad de Negocio general. Los planes de respuesta por actividad (en el nivel operativo) abordan la respuesta al incidente de cada departamento o unidad de negocio. Algunos ejemplos de los planes de respuesta por operación son:

- Procedimientos para ayudar a un equipo de respuesta a incidentes generalmente dirigido por un departamento que se ocupa del incidente específico y su impacto material (si existe)
- Una respuesta de recursos humanos a problemas de necesidades básicas durante un incidente

- Un plan del departamento para reiniciar actividades en un plazo predeterminado
- Una respuesta logística del departamento de TI a la pérdida y subsiguiente recuperación de los servicios de TI para el negocio

La complejidad y urgencia de los procesos de negocio pueden determinar si los planes operativos sólo se ocupan de una actividad o abarcan un departamento que gestiona varias actividades. Según el grado de complejidad de la organización, los planes de respuesta operativos pueden ser respaldados por planes más detallados para respuestas, ubicaciones o equipos específicos.

ETAPA 4 – PROBAR, MANTENER Y REVISAR

Garantiza que las estrategias, planes y acuerdos de GCN de la organización son refrendados por pruebas y revisiones, además de estar actualizados.

Pruebas

Conjunto de medidas que ponen a prueba el Plan de Continuidad de Negocios, los integrantes de los equipos y la tecnología y procedimientos. Se suelen utilizar tres términos:

- Prueba (Test): suelle referirse a someter a examen un proceso tecnológico o de negocio, generalmente con respecto al cumplimiento de ciertos plazos. Es posible que el resultado sea "pasa" o "falla" (para el proceso, no la persona). Un ejemplo podría ser la recuperación de un servidor mediante los archivos de respaldo.
- Simulacro: Práctica de un conjunto específico de procedimientos que requieren el seguimiento de un guión para inculcar conocimientos y familiarizarse con la práctica. Un ejemplo sería un simulacro de incendio.

- Ejercicio: Suelen realizarse para un evento basado en un escenario en el que se ponen a prueba la capacidad para tomar decisiones. Un ejemplo es un ejercicio de escritorio para gestionar un incidente grave.

El proceso de probar la GCN puede brindar los siguientes resultados:

- Comprobación de que la Continuidad de Negocio y las estrategias son efectivas.
- Grado de familiaridad del personal con sus funciones, responsabilidades y autoridad en respuesta a un incidente.
- Prueba de los aspectos técnicos, logísticos y administrativos del Plan de Continuidad de Negocio.
- Prueba de la infraestructura de recuperación como los centros de mando, el área de trabajo, tecnología y telecomunicaciones.
- Documentar los resultados del ejercicio en un informe posterior para la alta dirección, auditores, aseguradoras, autoridades y demás partes interesadas
- Documentar y resolver todas las cuestiones que han surgido en el ejercicio.
- Una conciencia mayor acerca de los procedimientos de emergencia.
- Una conciencia mayor acerca del significado de la GCN.
- La oportunidad para identificar las deficiencias y posibilidades de mejora en la preparación a la Continuidad de Negocio por parte de la organización

Mantenimiento

El proceso de mantenimiento de la Continuidad de Negocio brinda los siguientes resultados: un programa documentado de supervisión y mantenimiento de la Continuidad de Negocio, un informe de mantenimiento claramente definido (con recomendaciones) acordado y ratificado por el directivo adecuado, un plan de acción del informe de mantenimiento claramente definido acordado y ratificado por

el directivo adecuado, Planes de Continuidad de Negocio, estrategias y soluciones que sean efectivos y adecuados.

Revisar

La política acerca de la frecuencia de las auditorías debe estar claramente definida y estipulada en la "Política y Estándares de Auditoría" de la organización. Existen varias formas de revisar un programa de GCN: Auditoría interna, Auditoría externa, Autoevaluación.

4.4. ITIL

Information Technology Infraistructure Library (ITIL) es un marco de trabajo que define los mejores prácticas y enfoques de la gestión de Tecnologías de la Información (TI). Detalla la forma en que la Gestión de Servicios TI (ITSM) puede ser implementada en una empresa para mejorar la calidad de los servicios de TI por las personas que utilizan software, servicios y metodologías de forma colectiva. [10]. Su objetivo es mejorar la calidad de los servicios TI ofrecidos, evitar los problemas asociados a los mismos y en caso de que estos ocurran ofrecer un marco de actuación para que estos sean solucionados con el menor impacto y a la mayor brevedad posible.

Sus orígenes se remontan a la década de los 80 cuando el gobierno británico, preocupado por la calidad de los servicios TI de los que dependía la administración, solicito a una de sus agencias, la CCTA acrónimo de Central Computer and Telecommunications Agency, para que desarrollara un estándar para la provisión eficiente de servicios TI. En la actualidad es la OGC (Office of Government Commerce) el organismo encargado de velar por este estándar y la responsable de la última versión de ITIL (v3) que data del año 2007.

ITIL implementa diferentes procesos de Gestión de Servicios de TI, tales como la gestión del ciclo de vida y solicitud de gestión para mejorar la calidad de los servicios de TI. El componente básico contiene cinco estrategias de gestión del marco de ITIL, que representan el ciclo de vida de servicios de TI. Las diferentes estrategias de manejo son:

Figura 2. Ciclo de Vida de la Gestión de Servicio de TI- ITIL

- ***Estrategia del servicio.*** Ayuda a la compañía a planificar la implementación de estrategias de gestión de servicios de TI. Permite definir nuevos servicios de TI y ayudar a asegurar que la los servicios de TI actualmente establecidos satisfacen las necesidades de la empresa.

- ***Diseño del Servicio.*** Ayuda a crear políticas, arquitecturas y diseños para los servicios de TI para satisfacer las necesidades actuales y futuras de una empresa.

- ***Transición del Servicio.*** Ayuda a gestionar y controlar los cambios en los servicios de TI que se implementan en el entorno de trabajo de una empresa y asegurar la continuidad de los servicios de TI cuando se produzcan cambios.

- ***Operación del Servicio.*** Asegurar que los servicios de TI se ofrezcan efectiva y eficientemente. Esto incluye cumplir con los requerimientos de los usuarios,

resolver fallos en el servicio, arreglar problemas y llevar a cabo operaciones rutinarias del día a día.

- ***Mejora continua del servicio.*** Ayuda a lograr una mejor calidad de servicios de TI en una empresa, identificando y evaluando iniciativas, medidas correctivas y cumplimiento de metas que mejoren la efectividad y eficiencia de procesos y servicios de TI.

En la etapa de *Diseño del Servicio* se define el proceso ***Gestión de la Continuidad de los Servicios de TI (ITSCM),*** en el cual se establecen planes de contingencia que aseguren la continuidad del servicio en un tiempo predeterminado con el menor impacto posible en los servicios de carácter crítico. El objetivo de ITSCM es apoyar la continuidad, la gestión de procesos empresariales, asegurando las instalaciones que requiere servicios técnicos (incluyendo sistemas informáticos, redes, aplicaciones, repositorios de datos, telecomunicaciones, medio ambiente, apoyo técnico y mesa de servicios), reduciendo el riesgo de eventos desastrosos hasta niveles aceptables y planificando la recuperación en caso de que ocurran. ITSCM se centra en los eventos que la empresa considera lo suficientemente importantes como para ser considerado un desastre. Los eventos menos importantes se tratarán como parte del proceso de Gestión de Incidencias.

Figura 5. Procesos de la Gestión de Servicios de TI - ITIL

La **Gestión de la Continuidad del Servicio** se preocupa por impedir que una imprevista y grave interrupción de los servicios TI, debido a desastres naturales u otras fuerzas de causa mayor, tengan consecuencias catastróficas para el negocio.

Las siguientes secciones contienen detalles de cada una de las etapas en el ciclo de vida de ITSCM. [11]

Figura 6. Ciclo de vida de la Gestión de la Continuidad de los Servicios
Fuente: ITIL v.3 – Service Design

ETAPA 1 – INICIO

El proceso de iniciación cubre la totalidad de la organización y se compone de las siguientes actividades:

Configuración de Políticas. Debe ser establecido y comunicado tan pronto como sea posible para que todos los miembros de la organización involucrados o afectados por problemas de continuidad de negocio sean conscientes de sus responsabilidades para cumplir y apoyar ITSCM. Como mínimo, la política debe establecer la intención de la gestión y objetivos.

Especificar los términos de referencia y ámbito de aplicación. Incluye la definición del alcance y las responsabilidades de todo el personal de la organización. Abarca tareas como la realización de un Análisis de Riesgo y

Análisis de impacto en las empresas y la determinación de la estructura de mando y control necesarios para apoyar una interrupción del negocio. También es necesario tener en cuenta aspectos como los requisitos de los clientes, puntos pendientes de auditoría, reglamentaciones, condiciones de seguros y cumplimiento de las normas tales como ISO 27001 (que también se ocupa de los requisitos de continuidad de servicio).

Asignar recursos. El establecimiento de un eficaz medio de Continuidad de Negocio requiere recursos considerables en términos de dinero y mano de obra. Dependiendo de la madurez de la organización, con respecto a ITSCM, puede haber una obligación de conocer y/o capacitar al personal para llevar a cabo la Etapa 2. Como alternativa, el uso de consultores externos con experiencia puede ayudar a completar el análisis con mayor rapidez. Sin embargo, es importante que la organización pueda mantener el proceso en el futuro sin necesidad de depender totalmente de la ayuda externa.

Definir la organización del proyecto y la estructura de control. Los proyectos de ITSCM y BCM son potencialmente complejos y tienen que estar bien organizados y controlados. Se recomienda utilizar una reconocida metodología estándar de planificación del proyecto, PRCE o PMBOK.

Acuerdos del proyecto y planes de calidad. Los planes deben permitir que el proyecto sea controlado y administradas las desviaciones, asegurar que los servicios se consiguen en un nivel aceptable de calidad, proporcionar un mecanismo para comunicar las necesidades de recursos del proyecto y sus resultados finales, y así obtener la aprobación de todas las partes necesarias.

ETAPA 2 – REQUISITOS Y ESTRATEGIA

Conocer los requisitos de negocio para la continuidad del servicio es un componente crítico necesario para determinar qué tan bien la organización va a sobrevivir a un desastre o una interrupción y los costos en que se incurre. Si el análisis de los requisitos es incorrecto o la información clave ha sido perdida, podría tener graves consecuencias sobre la eficacia de los mecanismos de ITSCM. Esta etapa divide en dos secciones:

Requisitos – Análisis de impacto y evaluación de riesgos en la compañía.

Estrategia – Al realizar el análisis de los requisitos se establecen las medidas necesarias para reducir el riesgo y las estrategias de recuperación para apoyar el negocio.

Requisito – Análisis del impacto

El propósito de un Análisis de Impacto (BIA) es cuantificar el impacto que tendría el negocio debido a la pérdida de servicios. Este impacto podría ser un fuerte al ser identificado con exactitud, por ejemplo la pérdida financiera, o suave como las relaciones públicas, la salud moral y la seguridad o la pérdida de ventaja competitiva. En el BIA se identificarán los servicios más importantes para la organización y por lo tanto será el insumo clave para la estrategia.

El BIA identifica:

- El tipo de daño o pérdida, por ejemplo pérdida de ingresos, costos adicionales, daño en la reputación, pérdida de ventaja competitiva, incumplimiento de la ley, pérdida a largo plazo de la cuota de mercado, pérdida de la capacidad operativa (en un entorno de mando o control);
- El grado o nivel de daño después de la interrupción del servicio, y las horas del día, semana, mes o año en que la interrupción será más grave.

- La dotación de personal, las habilidades, las instalaciones y servicios (incluidos los servicios de TI) necesarios para los procesos críticos de negocio puedan seguir operando a un nivel mínimo aceptable.
- El tiempo en el que los niveles mínimos de dotación de personal, instalaciones y servicios deben ser recuperados.
- El tiempo en el que todos los procesos de negocio necesarios y personal de apoyo, instalaciones y servicios debe estar plenamente recuperados.
- La prioridad relativa de recuperación para cada uno de los servicios de TI.

Requisito – Análisis de Riesgos

El propósito de un Análisis de Riesgos en ITSCM es determinar la probabilidad de que realmente ocurra un desastre o una interrupción grave de los servicios. Se trata de una evaluación del nivel de una amenaza y el grado en que una organización es vulnerable a ella. Puede utilizarse para evaluar y reducir la probabilidad de incidentes normales de funcionamiento. Se recomienda utilizar una metodología estándar de Administración de Riesgo.

Figura 8. Proceso de Administración de Riesgos

Se deberá identificar las amenazas y oportunidades que podrían afectar la capacidad de alcanzar el objetivo de una actividad, evaluar el efecto neto de las amenazas detectadas y las oportunidades asociadas a una actividad, preparar una respuesta específica que reduzca las amenazas y maximizar las oportunidades, poner en práctica las acciones y supervisar su efectividad, tomar medidas correctivas cuando las respuestas no coinciden con las expectativas, revisar y mejorar las acciones para asegurar que siguen siendo eficaces, garantizar que todo el mundo se mantenga al día con los cambios en las amenazas, oportunidades y otros aspectos de la gestión de cualquier riesgo.

Estrategia – Continuidad

El resultado de los análisis de impacto y de riesgos permitirá definir estrategias de continuidad acordes con las necesidades del negocio. La estrategia deberá tener un equilibrio óptimo entre la reducción de riesgos, recuperación y opciones de continuidad. Se quiere concentrar los esfuerzos de reducción de riesgos en los servicios que han sido identificados como de alto impacto en el corto plazo dentro de BIA, por ejemplo, a través de la resistencia total y la tolerancia a fallos.

Opciones de Recuperación

La estrategia a seleccionar debe ser un equilibrio entre el costo de las medidas de reducción de riesgos y las opciones de recuperación para apoyar los procesos críticos de negocio dentro de los plazos acordados. La siguiente es una lista de las posibles opciones de recuperación de TI que necesitan ser considerados en el desarrollo de la estrategia:

- Trabajo Manual. Para ciertos tipos de servicios, puede ser una medida eficaz provisional durante un tiempo limitado hasta que el servicio de TI se reanude.

- Recuperación Gradual. Es llamada *Cold standby*, incluye la provisión de un sitio alterno vacío, totalmente equipado con electricidad, controles ambientales, infraestructura de red, cableado, conexiones de telecomunicaciones, y está disponible para la compañía en una situación de desastre para instalar su propio equipo informático. No incluye los equipos informáticos actuales, por lo que no es aplicable a los servicios que requieren pronta recuperación, esta opción sólo se recomienda para los servicios que puede soportar un retraso de tiempo de recuperación en días o semanas, no en horas.
- Recuperación Intermedia. Es llamada *Warm standby*, requiere un sitio alterno con sistemas activos diseñados para recuperar los servicios críticos en un plazo de entre 24 y 72 horas. La ventaja de esta opción es que el cliente puede tener acceso al sitio prácticamente al instante, ubicado en un edificio seguro, sin embargo, el restablecimiento de los servicios puede tomar algún tiempo, ya que los retrasos se pueden encontrar mientras se vuelve a configurar las aplicaciones y restaurar los datos de las copias de seguridad.
- Recuperación Rápida. Es llamada *Hot standby*, requiere un sitio alterno con una replicación continua de datos y con todos los sistemas activos preparados para la inmediata sustitución del ambiente de producción. Ésta es evidentemente la opción más costosa y debe emplearse sólo en el caso de que la interrupción del servicio TI tuviera inmediatas repercusiones comerciales. La instalación tiene que estar ubicada por separado y lo suficientemente lejos para no se vea afectado por una catástrofe que afecte a esa ubicación.

ETAPA 3 – IMPLEMENTACION

El Plan de ITSCM debe contener toda la información necesaria para recuperar los sistemas informáticos, redes y telecomunicaciones en una situación de desastre una vez presentada, y para gestionar el retorno al funcionamiento normal luego que la interrupción del servicio se ha resuelto. Se debe elaborar una serie de documentos entre los que se incluyen

- Plan de prevención de riesgos. Su objetivo principal es el de evitar o minimizar el impacto de un desastre en la infraestructura TI.
- Plan de gestión de emergencias. deben tener en cuenta aspectos como: evaluación del impacto de la contingencia en la infraestructura TI, asignación de funciones de emergencia al personal del servicio TI, comunicación a los usuarios y clientes de una grave interrupción o degradación del servicio, procedimientos de contacto y colaboración con los proveedores involucrados, protocolos para la puesta en marcha del plan de recuperación correspondiente.
- Plan de recuperación. Debe incluir todo lo necesario para: reorganizar al personal involucrado, restablecer los sistemas de hardware y software necesarios, recuperar los datos y reiniciar el servicio TI. Además, involucran: asignación de personal y recursos, instalaciones y hardware alternativos, Planes de seguridad que garanticen la integridad de los datos, procedimientos de recuperación de datos, Contratos de colaboración con otras organizaciones, Protocolos de comunicación con los clientes.

ETAPA 4 – OPERACIÓN EN CURSO

Esta etapa consistirá en lo siguiente:

- *Educación, sensibilización y formación*. Es indispensable que la ITSCM: dé a conocer al conjunto de la organización TI los planes de prevención y recuperación, ofrezca formación específica sobre los diferentes procedimientos de prevención y recuperación, realice periódicamente simulacros para diferentes tipos de desastres con el fin de asegurar la capacitación del personal involucrado, facilite el acceso permanente a toda la información necesaria.
- *Revisión*. Periódicamente revisar que todos los entregables del proceso ITSCM para asegurar que siguen siendo actuales.
- *Pruebas*. Es necesario establecer un programa de pruebas periódicas para garantizar que los componentes críticos de la estrategia se ponen a prueba, de preferencia al menos una vez al año, aunque las pruebas de Planes de Continuidad de Servicios de TI deben ser dispuestos de acuerdo con las necesidades del negocio y las necesidades de los BCP.
- *Gestión de Cambios*. Todos los planes también deben ser examinados después de cada cambio en los procesos principales. Cualquier cambio en la tecnología de TI también se debe incluir en la estrategia, para asegurar que después de un desastre funcione correctamente dentro de la prestación de servicios de TI.
- *Invocación*. Una interrupción puede ocurrir en cualquier momento del día o noche, por lo que es esencial que la guía del proceso de invocación esté disponible dentro y fuera de la oficina para el equipo de gestión de riegos. La decisión de invocar debe hacerse rápidamente para ahorrar tiempo en las

habilitaciones de servicios en el sitio de recuperación, y no debe tomarse a la ligera si se va a utilizar un sitio de terceros por los costos y periodos determinados para el uso de las instalaciones. El periodo de retorno a la normalidad debe ser cuidadosamente planificado y realizado de manera controlada, es importante que todo el personal que sean consciente de sus responsabilidades para asegurar una transición sin problemas.

INDICADORES CLAVE DE RENDIMIENTO

KPI (Métrica de CSI)	Descripción
Procesos de negocio con acuerdos de continuidad	Porcentaje de procesos de negocio cubiertos por metas específicas de continuidad del servicio
Lagunas en preparación para desastres	Cantidad de lagunas identificadas en la preparación para eventos de desastres (amenazas serias sin contramedidas definidas)
Duración de la implementación	Duración desde la identificación del riesgo relacionado a desastres hasta la implementación de un mecanismo de continuidad adecuado
Cantidad de prácticas para desastres	Cantidad de prácticas para desastres que realmente se llevaron a cabo
Cantidad de defectos identificados durante las prácticas para desastres	Cantidad de defectos identificados en la preparación para eventos de desastres identificados durante las prácticas

4.5. COBIT

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los interesados (Stakeholders). Permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas; constantemente se actualiza y armoniza con otros estándares, por lo tanto, se ha convertido en el integrador de las mejores prácticas de TI y marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. [10]

En COBIT se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI. Estos procesos están agrupados en cuatro grandes dominios que son: *PLANEAR Y ORGANIZAR (PO), ADQUIRIR E IMPLEMENTAR (AI), ENTREGAR Y DAR SOPORTE (DS), MONITOREAR Y EVALUAR (ME).*

El domino *ENTREGAR Y DAR SOPORTE* cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas. Dentro de este dominio se define el proceso *DS4 - ASEGURAR LA CONTINUIDAD DEL SERVICIO* donde se tienen actividades que van desde la creación del marco de referencia para la continuidad de las operaciones y la definición de una estrategia y filosofía de continuidad hasta las indicaciones de contenido, implementación, prueba y distribución del mismo.

PROCESO DS4 - GARANTIZAR LA CONTINUIDAD DEL SERVICIO

La necesidad de brindar continuidad a los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.

Las entradas del proceso son:

Figura 6. Entradas del Proceso DS4 – Garantizar la Continuidad del Servicio

Fuente: Cobit 4.1

Las salidas del proceso son:

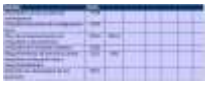


Figura 7. Salidas del Proceso DS4 – Garantizar la Continuidad del Servicio

Fuente: Cobit 4.1

Los roles y responsabilidades para la ejecución efectiva y eficiente de las actividades clave y su documentación, así como la rendición de cuentas para los entregables finales del proceso, son los siguientes:

Figura 8. Matriz RACI del Proceso DS4 – Garantizar la Continuidad del Servicio

Fuente: Cobit 4.1

OBJETIVOS DE CONTROL

Los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI. Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo, consisten en políticas, procedimientos, prácticas y estructuras organizacionales; están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

Los objetivos de control del proceso Garantizar la Continuidad del Servicio son:

DS4.1 - Marco de Trabajo de Continuidad de TI

Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomen cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

DS4.2 - Planes de Continuidad de TI

Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

DS4.3 - Recursos Críticos de TI

Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.

DS4.4 - Mantenimiento del Plan de Continuidad de TI

Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.

DS4.5 - Pruebas del Plan de Continuidad de TI

Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.

DS4.6 - Entrenamiento del Plan de Continuidad de TI

Asegurarse de que todas las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.

DS4.7 - Distribución del Plan de Continuidad de TI

Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre.

DS4.8 - Recuperación y Reanudación de los Servicios de TI

Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio.

DS4.9 - Almacenamiento de Respaldos Fuera de las Instalaciones

Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos

de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

DS4.10 - Revisión Post Reanudación

Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

METAS Y METRCAS

Es claro que los procesos requieren controles, los cuales son los que brindan la seguridad de que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos. Es así como para cada proceso se debe recoger información de control, la cual se debe comparar con una métrica y a partir del resultado se deberá actuar para obtener el mayor beneficio.

Se definen en COBIT en tres niveles:

- Las metas y las métricas de TI, que definen lo que el negocio espera de TI.
- Las metas y las métricas de Procesos, que definen lo que el proceso de TI debe generar para dar soporte a los objetivos de TI.
- Las metas y las métricas de las Actividades, que facilitan el desempeño efectivo de los procesos.

Las metas y las métricas del Proceso DS4 - GARANTIZAR LA CONTINUIDAD DEL SERVICIO, se detallan en la siguiente tabla:

	TI	PROCESOS	ACTIVIDADES
METAS	- Asegurar que los servicios de TI estén disponibles según se requieran. - Asegurar un mínimo impacto al negocio en caso de una interrupción o cambio en los servicios de TI. - Asegurar que los servicios y la infraestructura de TI puedan resistir y recuperarse de fallas originadas por un error, ataque deliberado o desastre.	- Establecer un plan de continuidad de TI que soporte los planes de continuidad del negocio. - Desarrollar planes de continuidad de TI que puedan ejecutarse, probarse y mantenerse. - Minimizar la posibilidad de interrupción de los servicios de TI.	- Desarrollar y mantener (mejorar) los planes de contingencia de TI. - Habilitación y pruebas de los planes de contingencia. - Almacenamiento de copias de los planes de contingencia fuera de las instalaciones.
MÉTRICAS	- # de horas perdidas por usuario por mes debido a interrupciones no planeadas	- % de SLAs de disponibilidad que se cumple - # de procesos críticos del negocio que dependen de TI, no cubiertos por un plan de continuidad - % de pruebas para lograr los objetivos de recuperación - Frecuencia en la interrupción de servicios de sistemas críticos	- Tiempo transcurrido entre las pruebas de cualquier elemento dado del plan de continuidad de TI - Número de fases de habilitación por año de cada elemento relevante de TI - % de componentes de infraestructura críticos con monitoreo de disponibilidad automatizado - Frecuencia de revisión del plan de continuidad de TI.

Fuente: COBIT 4.1

MODELO DE MADUREZ

Los modelos de madurez ayudan a los directivos de las organizaciones a identificar que tan bien se está administrando TI, es un método que permite evaluar desde un nivel 0-No existente hasta el nivel 5-Optimizado. En él se podrá identificar: el desempeño real de la empresa, el estatus actual de la industria y el objetivo de mejora de la empresa.

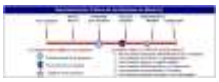


Figura 9. Modelo de Madurez del Proceso DS4 – Garantizar la Continuidad del Servicio
Fuente: Cobit 4.1

EL modelo de madurez del proceso Garantizar la Continuidad del Servicio es:

0 - No Existente

Cuando no hay entendimiento de los riesgos, vulnerabilidades y amenazas a las operaciones de TI o del impacto en el negocio por la pérdida de los servicios de TI. No se considera que la continuidad en los servicios deba tener atención de la gerencia.

1 - Inicial / Ad Hoc

Cuando las responsabilidades sobre la continuidad de los servicios son informales y la autoridad para ejecutar responsabilidades es limitada. La gerencia comienza a darse cuenta de los riesgos relacionados y de la necesidad de mantener continuidad de los servicios. El enfoque de la gerencia sobre la continuidad del servicio radica en los recursos de infraestructura, en vez de radicar en los servicios de TI. Los usuarios utilizan soluciones alternas como respuesta a la interrupción de los servicios. La respuesta de TI a las interrupciones mayores es reactiva y sin preparación. Las pérdidas de energía planeadas están programadas para cumplir con las necesidades de TI pero no consideran los requerimientos del negocio.

2 - Repetible pero Intuitivo

Cuando se asigna la responsabilidad para mantener la continuidad del servicio. Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio. No hay un plan de continuidad de TI documentado, aunque hay compromiso para mantener disponible la continuidad del servicio y sus principios más importantes se conocen. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable. Las prácticas de continuidad en los servicios emergen, pero el éxito depende de los individuos.

3 - Definido

Cuando la responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas. El plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto al negocio. Hay reportes periódicos de las pruebas de continuidad. Los individuos toman la iniciativa para seguir estándares y recibir habilitación para

enfrentarse con incidentes mayores o desastres. La gerencia comunica de forma regular la necesidad de planear el aseguramiento de la continuidad del servicio. Se han aplicado componentes de alta disponibilidad y redundancia. Se mantiene un inventario de sistemas y componentes críticos.

4 - Administrado y Medible

Cuando se hacen cumplir las responsabilidades y los estándares para la continuidad de los servicios. Se asigna la responsabilidad de mantener un plan de continuidad de servicios. Las actividades de mantenimiento están basadas en los resultados de las pruebas de continuidad, en las buenas prácticas internas y en los cambios en el ambiente del negocio y de TI. Se recopila, analiza y reporta documentación estructurada sobre la continuidad en los servicios y se actúa en consecuencia. Se brinda habilitación formal y obligatoria sobre los procesos de continuidad. Se implementan regularmente buenas prácticas de disponibilidad de los sistemas. Las prácticas de disponibilidad y la planeación de la continuidad de los servicios tienen influencia una sobre la otra. Se clasifican los incidentes de discontinuidad y la ruta de escalamiento es bien conocida por todos los involucrados. Se han desarrollado y acordado KGIs y KPIs para la continuidad de los servicios, aunque pueden ser medidos de manera inconsistente.

5 - Optimizado

Cuando los procesos integrados de servicio continuo toman en cuenta referencias de la industria y las mejores prácticas externas. El plan de continuidad de TI está integrado con los planes de continuidad del negocio y se le da mantenimiento de manera rutinaria. El requerimiento para asegurar continuidad es garantizado por los proveedores y principales distribuidores. Se realizan pruebas globales de continuidad del servicio, y los resultados de las pruebas se utilizan para actualizar el plan. La recopilación y el análisis de datos se utilizan para mejorar continuamente el proceso. Las prácticas de disponibilidad y la continua

planeación de la continuidad están completamente alineadas. La gerencia asegura que un desastre o un incidente mayor no ocurrirán como resultado de un punto único de falla. Las prácticas de escalamiento se entienden y se hacen cumplir a fondo. Los KGIs y KPIs sobre el cumplimiento de la continuidad de los servicios se miden de manera sistemática. La gerencia ajusta la planeación de continuidad como respuesta a los KGIs y KPIs.

4.6. MAPEO DE LOS OBJETIVOS DE CONTROL DE COBIT 4.1 CON ITIL v 3

Para determinar dónde encajan los componentes de COBIT e ITIL con los planes de Continuidad de TI, presentamos a continuación la siguiente tabla.

Al igual que la mayoría de normas, prácticas y marcos actuales, COBIT e ITIL son metódicos. Ellos describen "qué" hay que hacer, pero no "cómo" hacerlo. Se puede utilizar la tabla como una lista de comprobación para asegurar que no se ha omitido ninguna de las actividades principales.

Las pruebas y los ejercicios de los planes de Continuidad de TI se encuentran entre las actividades más importantes en el proceso. Por ejemplo, el punto DS4.5 de COBIT señala: "Realice pruebas del plan de continuidad de TI de forma regular para garantizar que los sistemas pueden ser recuperados de manera efectiva, que las deficiencias son atendidas y que el plan sigue siendo aplicable. Esto requiere una cuidadosa preparación, documentación, elaboración de informes sobre los resultados de las pruebas y, de acuerdo con los resultados, la aplicación de un plan de acción. Evalúe el alcance de las pruebas de recuperación de aplicaciones individuales en escenarios de pruebas integrados, en pruebas de extremo a extremo y en pruebas integradas con los proveedores".

Por el contrario, si analizamos las previsiones de ITIL, vemos que ITIL avala un marco de trabajo denominado Gestión de la Continuidad del Servicio de TI (ITSCM TI Service Continuity Management). El ITSCM se ocupa de los riesgos que podrían causar un impacto repentino y grave en la infraestructura de TI, de manera que una interrupción de los mismos podría poner en peligro la continuidad del funcionamiento de la empresa. De acuerdo con ITIL, la ITSCM debe estar alineada con el ciclo de vida de continuidad del negocio. La ITSCM se centra en la protección de la infraestructura tecnológica, mientras que la continuidad del negocio se centra en los riesgos que podrían interrumpir las operaciones de negocio. Los puntos SD 4.5.5.3 y SD 4.5.5.4 se ocupan de los enfoques y de las actividades y técnicas que hacen posible la ITSCM. También describen las medidas de planificación, protección y optimización de las etapas 3 y 4,

Implementación (SD 4.5.5.3) y Operación en curso (SD 4.5.5.4), del ciclo de vida de la ITSCM.

En este caso, las guías de COBIT y de ITIL pueden ser utilizadas como parte del proceso de prueba de continuidad y recuperación ante desastres de TI. En el punto 4.1 de COBIT se dan detalles más específicos sobre los objetivos de una prueba. Por su parte, ITIL dibuja los procesos básicos de gestión sin entrar en detalles tan específicos.

Las organizaciones que deseen adoptar las buenas prácticas para las operaciones de TI, incluyendo la Continuidad de TI, pueden beneficiarse con la utilización de estos marcos de gestión. Los marcos proporcionan unos enfoques coherentes y medibles. También tienen más posibilidades de garantizar un resultado exitoso, especialmente tras una interrupción no planificada de los servicios de TI.

5. ALCANCES Y LIMITACIONES

Los alcances de este proyecto consisten básicamente en lograr diseñar un Marc o Metodológico para el desarrollo de un plan de continuidad, en un plazo de tiempo de cuatro meses aproximadamente, que incluye las fases de Diagnóstico, Diseño y presentación del Marco. Este proyecto no abarca la implementación del marco metodológico, pero se van incluir ejemplos y procesos claves que ilustren la estructura del plan.

6. METODOLOGIA

El marco metodológico se desarrollará haciendo un recorrido detallado del estándar BS 25999, el proceso Gestión de la Continuidad de los Servicios de TI de ITIL y el proceso "DS4 - Asegurar la continuidad del servicio" del dominio "Entrega y soporte" de COBIT, con el propósito de precisar e identificar las áreas y fases a tratar en el marco metodológico a proponer. Despues de esto, consideramos que para cumplir con los objetivos o dar respuesta concreta al problema identificado se deben aplicar la investigación, observación, análisis y síntesis en las siguientes etapas:

Etapa 1: Interpretación de los diferentes estándares. Consiste en la lectura, análisis y síntesis de BS - 25999, ITIL y COBIT. En este caso se realizará una seria investigación y levantamiento de información adicional que permita el - entendimiento de los Procesos.

Etapa 2: Formulación del proyecto. Consistirá en la definición y detalle de las metas en tiempo, espacio, objetivos y alcances.

Etapa 3: Definición de un marco metodológico compuesto por diferentes fases y actividades. Consistirá en la identificación de las principales fases y actividades, y determinar las herramientas que se necesitarán para seguir las pautas del marco de trabajo.

Etapa 4: Diseño de la Herramienta. En esta etapa se realizará el diseño de la herramienta, teniendo en cuenta las fases y actividades de un Plan de Continuidad del Negocio.

7. IMPACTOS Y RESULTADOS ESPERADOS

Este proyecto surge como una necesidad del sector empresarial, y proporcionará un marco metodológico o una guía práctica para que el personal de TI, implemente de manera ágil un Plan de Continuidad del Negocio que permita prevenir o evitar los posibles escenarios originados por una situación de crisis así como minimizar las consecuencias económicas, reputacionales o de responsabilidad civil derivadas de la misma, y que ayude a reducir los costos asociados a la interrupción o evitar penalizaciones contractuales por incumplimiento de contratos como proveedor de productos o servicios.

8. MARCO METODOLÓGICO PROPUESTO

En primera instancia una representación gráfica de las fases que componen el marco metodológico para el desarrollo de un Plan de Continuidad propuesto en el cual se distinguen 6 fases secuenciales que son:

Figura 10. Diagrama de Fases del Plan de Continuidad

8.1. DISEÑAR LA POLITICA

Comprende la identificación de las actividades que deben ser realizadas de forma previa para comenzar el proceso de desarrollo e implantación del Plan de Continuidad. Es indispensable contar con el apoyo de la Alta Dirección así como la inversión económica necesaria. Las actividades a realizar son las siguientes:

ACTIVIDAD 1. Establecer los responsables de la Continuidad del Negocio. Es necesario designar un coordinador quien se encargue gestionar y supervisar el proceso de elaboración del plan. Es recomendable constituir (dependiendo de la inversión) un equipo de continuidad del negocio.

ACTIVIDAD 2. Elaborar la política de continuidad. La política se entiende como un documento sencillo, claro y conciso que establece a alto nivel (estratégico) los objetivos, el alcance y las responsabilidades en la gestión de la continuidad de negocio en la organización.

ACTIVIDAD 3. Planificar el proyecto. El coordinador o equipo de continuidad debe aplicar sus habilidades de gestión de proyectos para programar y desarrollar el plan de trabajo, que incluye: tareas a llevar a cabo, responsables de ejecutar las tareas, tiempos de ejecución, hitos, presupuestos, plazos e indicadores de éxito.

8.2. ANALIZAR LOS RIESGOS

En el desarrollo de este proyecto, nos basaremos en la Norma Técnica Colombiana – NTC5254, la cual es una adopción idéntica de la AS/NZ 4360 y que provee un instructivo genérico para el establecimiento e implementación el proceso de administración de riesgos involucrando la determinación del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos. Esta guía hace un recorrido a los riesgos, empezando desde su tratamiento e identificación hasta el monitoreo y revisión, lo que le permite a la organización una administración efectiva de los riesgos tanto para evitar o mitigar las posibles pérdidas como para aprovechar las oportunidades que hay en el entorno.

Los principales elementos de la gestión de riesgos, son los siguientes:

Comunicación y Consulta. Comunicar y consultar con las partes involucradas, internas y externas, según sea adecuado, en cada etapa del proceso de gestión de riesgo y relacionadas en el proceso como un todo.

Establecimiento del Contexto. Establecer el contexto interno y externo de la gestión de riesgo en el cual tendrá lugar el resto del proceso. Se recomienda establecer los criterios frente a los cuales se evaluará el riesgo y definir la estructura del análisis.

Identificación de los riesgos. Identificar dónde, cuándo, por qué y cómo podrían los eventos prevenir, degradar, retardar o potenciar el logro de los objetivos.

Análisis de los Riesgos. Identificar y evaluar los controles existentes. Determinar las consecuencias y la posibilidad y por ende el nivel de riesgo. En este análisis se deberá tener en cuenta el rango de consecuencias potenciales y cómo estas podrían ocurrir.

Evaluación de los Riesgos. Comparar los niveles estimados de riesgo frente a los criterios preestablecidos y considerar el equilibrio entre beneficios potenciales y resultados adversos. Esto permite tomar decisiones sobre el grado y la naturaleza de los tratamientos requeridos y sobre las prioridades.

Tratamiento de los Riesgos. Desarrollar e implementar estrategias específicas eficaces en términos de costos y planes de acción para incrementar los beneficios potenciales y reducir las pérdidas potenciales.

Monitoreo y Revisión. Es necesario monitorear la eficacia de todas las etapas del proceso de gestión de riesgo. Esto es importante para la mejora continua. Es necesario monitorear los riesgos y la eficacia de las medidas de tratamiento para asegurar que las circunstancias cambiantes no alteran las prioridades.

Figura 111. Proceso de Gestión de Riesgos en detalle

Fuente: NTC-ISO/IEC 27001

Se recomienda revisar la ISO/IEC 27005:2008, la cual proporciona una guía, e incluye los conceptos incluidos en ISO 27001 para ayudar en la tarea de gestión de la seguridad de la información basada en una aproximación de gestión de riesgos. La norma ha sido diseñada para ayudar a la puesta en práctica satisfactoria del análisis y la gestión del riesgo, fase principal del diseño de todo buen sistema de gestión de la seguridad de la información (SGSI). Es aplicable a todas los tipos de organizaciones que consideren importante su información, y permite conocer y gestionar los riesgos de dicha información vital para la Organización, frente a amenazas internas o externas.

El análisis de riesgos consiste en identificar las amenazas sobre estos activos y su probabilidad de ocurrencia, las vulnerabilidades asociadas a cada activo y el impacto que las citadas amenazas pueden provocar sobre la disponibilidad de los mismos. Dentro del Análisis de Riesgos podemos distinguir las siguientes actividades:

ACTIVIDAD 1. Identificar Activos. Para cada uno de los procesos críticos de la compañía es necesario realizar un inventario de los activos involucrados en el proceso. Los activos se definen como los recursos de una compañía que son necesarios para la consecución de sus objetivos de negocio. El proceso de elaborar un inventario de activos es uno de los aspectos fundamentales de un correcto análisis de riesgos. En este inventario se identificará claramente su propietario y su valor para la organización, así como su localización actual.
En la Herramienta de Análisis de Impacto, se obtiene gran parte de esta información, sobre los activos que componen los procesos críticos.

ACTIVIDAD 2. Identificar Amenazas. Una amenaza se define como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus servicios. A la hora de analizar los riesgos hay que evaluar las distintas amenazas que pueden provenir de las más diversas fuentes. Entre éstas se incluyen los agresores maliintencionados, las amenazas no intencionadas y los desastres naturales. La siguiente ilustración clasifica las distintas amenazas a los sistemas.

Figura 122. Clasificación Generación Amenazas

Es necesario identificar, entender y evaluar el riesgo de TI considerando todo lo que puede salir mal con o en relación a TI, usando para ello escenarios de riesgo, los cuales contienen varios components. La siguiente ilustración clasifica los distintos escenarios de riesgo.

Figura 132. Escenarios de Riesgo

ACTIVIDAD 3. Evaluar Vulnerabilidades. Las vulnerabilidades son debilidades que pueden ser explotadas para convertir una amenaza en un riesgo real que puede causar daños graves en una compañía. Las vulnerabilidades en sí mismas no causan daño alguno, sino que es una condición o un conjunto de condiciones que pueden permitir a una amenaza afectar a un activo. Para identificar las vulnerabilidades que pueden afectar a una compañía debemos responder a la pregunta, ¿Cómo puede ocurrir una amenaza? Para responder a esta pregunta ponemos como objetivo la amenaza y definimos las distintas situaciones por las que puede ocurrir la misma, evaluando si dentro de la compañía puede darse esa circunstancia; es decir, si el nivel de protección es suficiente para evitar que se materialice la amenaza. Por ejemplo: si nuestra amenaza es que nos roben datos estratégicos de la compañía, podemos establecer, entre otras, las preguntas: *¿Existen perfiles de acceso a las aplicaciones y datos? ¿Están los dispositivos de almacenamiento protegidos y controlados de forma adecuada?* Si no se responde afirmativamente a las preguntas, es que existen vulnerabilidades que podrían

utilizarse de forma que la amenaza se convierta en un incidente real, y causar daños importantes en la compañía.

ACTIVIDAD 4. Evaluar Riesgos. Independientemente de la metodología o de las herramientas empleadas para el análisis de riesgos, el resultado del proceso será un mapa de riesgos que permita identificar y priorizar aquellos que pueden provocar una paralización de las actividades de negocio de la organización o de los recursos críticos sobre los cuales dichas actividades están soportadas. Es habitual que las organizaciones adopten procesos de gestión de riesgos que generan matrices de análisis complejas de desarrollar y mantener, perdiendo la visión y el "sentido común" necesario para determinar en última instancia qué riesgos deben ser tomados en consideración.
El riesgo suele expresarse en términos cualitativos (Alto, Medio, Bajo). El sistema de evaluación propuesto es:

- 0 - No existe amenaza percibida de esta fuente.
- 1 - La amenaza existe, pero su ocurrencia es poco frecuente.
- 2 - Se trata de una amenaza inmediata que puede ocurrir en cualquier momento.

ACTIVIDAD 5. Medidas de Reducción de Riesgos. Los mecanismos preventivos reducir la posibilidad de que una compañía sufra una contingencia grave o un desastre y, si éste se produce, disminuir el daño que provocaría (aunque la organización no pueda evitar la caída de la energía eléctrica por una avería de su compañía de suministro, sí puede habilitar baterías o fuentes de alimentación alternativas e independientes que garanticen el suministro eléctrico durante un periodo de tiempo). Para reducir riesgos se utilizan los denominados

controles o medidas de seguridad. Existen diferentes opciones para hacer frente a los mismos:

- *Aceptar el riesgo*: la organización conoce el riesgo y decide asumirlo sin tomar ninguna acción al respecto, bien porque no tiene capacidad o bien porque el coste para mitigar el riesgo es desproporcionado para los beneficios que aporta.
- *Transferir el riesgo*: por ejemplo a través de la subcontratación de servicios o mediante la contratación de un seguro de cobertura, de forma que si el riesgo se materializa exista una compensación externa que lo mitigue.
- *Reducir el riesgo* a niveles aceptables por la organización: mediante el diseño y la implantación de controles o medidas preventivas o que atenúen los impactos y las consecuencias del mismo.
- *Evitar el riesgo*: mediante la eliminación del mismo (por ejemplo a través de la reingeniería de procesos o incluso suspendiendo la actividad que origina el riesgo sin penalizar los objetivos de negocio de la organización).

Algunas de las medidas típicas de reducción de riesgo incluyen: instalación de UPS y la energía de reserva para equipos, sistemas de alta disponibilidad para aplicaciones críticas donde incluso el tiempo de inactividad mínima es inaceptable (ej. un sistema bancario), RAID y duplicación de discos para servidores para prevenir la pérdida de datos, equipos y componentes de repuesto que se utilizarán en caso de fallo, sistemas y redes resistentes, contratación de servicios de outsourcing a más de un proveedor, aplicar controles de seguridad física y a TI, sistemas de detección de incendios junto con sistemas de extinción, establecer estrategia de copia de seguridad y recuperación de datos incluyendo el almacenamiento fuera del sitio, Monitorización de eventos, Auditorías internas, Revisiones periódicas de procesos, Detección de virus (Antivirus).

Estas medidas no necesariamente van a resolver o eliminar totalmente el riesgo, pero todos o una combinación de ellos puede reducir significativamente el riesgo asociado a la forma en que se prestan los servicios a la empresa.

HERRAMIENTA DE ANALISIS DE RIESGOS

Instrucciones
Cada pregunta debe ser considerada y debidamente sopesada antes de asignar una calificación
Si es evidente que el conocimiento sobre el tema es incompleto, utilice una calificación de 2 para resaltar el área de investigación
La técnica sugerida en el presente documento se ofrece como un conjunto de directrices, que pueden no ser totalmente completas. Su eficacia dependerá de la capacidad del usuario para evaluar e integrarlas en su entorno operativo propio.
Cualquier información introducida en este documento es confidencial y debe ser tratada como tal. Este documento se centra en determinados tipos de procesos que son riesgos.
consumo y la mayoría de organizaciones, los riesgos que potencialmente se consideran dentro de una inspección periódica se agrupan bajo los siguientes títulos o tipos de amenaza: Fuego, seguridad, Almacenamiento, Inundación, Peligros, Explosiones, Recursos, Comunicaciones, Protección de datos, Planes de Contingencia.
Finalmente, el propósito no es generar una puntuación, sino identificar aquellas áreas donde se requiere de estos y se deben tomar acciones para transferir, reducir o evitar el riesgo.

Sistema de Evaluación	
0 - No existe amenaza percibida de esta fuente	
1 - Se interesa existe, pero su ocurrencia es poco frecuente	
2 - Se trata de una amenaza inmediata que puede ocurrir en cualquier momento	

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

INCENDIO	Valoración
Incidente	
La alarma de incendio del edificio está conectada directamente al servicio local de bomberos?	
Tiene detectores de humo instalados?	
Los detectores de humo pueden funcionar si falla en fuente de luz?	
Tiene un sistema adicional de extinción automático?	
Están los extintores ubicados de manera visible y accesible?	
Hay algún empleado entrenado en utilizar los extintores disponibles en su sitio?	
Hay señales de incendio tanto del edificio (EL asambleo y Salidas Emergencia)?	
Hay un botiquín de incendios disponible?	
Ha habido en el entorno de evacuación de incendios durante los últimos seis meses?	
Se Preparo a cabo simulacros de incendio bajo la supervisión de un jefe de bomberos local?	
Si es así, todos el personal supo la secuencia de evacuación de incendios?	
Si apagan todos las luces por ejemplo, ¿todavía el edificio está bien ocupado?	
Cuando los alarmas suenan, ¿todos los ocupantes del incendio son conscientes con la ruta correcta?	
ATAQUE CIBERNÉTICO (Internet/Intranet)	
Hay políticas y procesos de peligro de inundación, tales, que se necesita para la salud o amenazar su edificio?	
ROBO/VANDALISMO	
En el edificio o sobre todo con el edificio de un mundo?	
Es el mismo de empleados	
Hay un centro de monitoreo cerca de sus instalaciones?	

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

RECURSOS	Calificación
Personal	
La seguridad perimetral del personal es la primera protección?	
La seguridad de las edificios es el segundo escalón?	
Otro seguridad en la zona de recepción?	
Existe un plan de seguridad física?	
El personal tiene los elementos de higiene personal en el trabajo?	
Esta permitido el acceso al personal de seguridad a sus oficinas?	
Se entrega el debido kardex en la toma de turnos y cambios de puestos?	
Los turnos de rondas son acudes por todos los empleados que la empresa?	
Efectúa un proceso de terminación formal que incluya la toma de firmas a ser desvinculados a la compañía (como Fuero, Tarjetas de identificación y acceso, etc)?	
Existe control de entrada y salida físicos a Personal visitas de terceros?	
Existe control de vehículos?	
Circuito cerrado?	
Esta contratado directamente a los servicios de emergencia?	
Existe la posibilidad de robo con violencia o robo a mano armada?	
Incendio	
Tiene hornos o cocinas en todas las viviendas?	
Tiene calentadores en todas las viviendas?	
Existe cerca o perimetro seguro de la propiedad con la vecina?	
Los otros alrededores el edificio se encuentra en fábrica de productos que impliquen que alguno pueda	
presentar incendio en una de las viviendas?	
Hay sistema de seguridad fuera del edificio?	
Hay sistema de seguridad dentro de las instalaciones?	
Existe un plan de evacuación de personal en caso de incendio para prevenir daños?	
Y en las vías de las instalaciones?	

DESASTRES NATURALES	Calificación
Tiene una copia de seguridad periódica de todos los datos y programas informáticos?	
Tiene copias de seguridad de los manuales técnicos/usuarios y la documentación?	
Conserva los datos, programas y documentación fuera instalaciones de la empresa que son vitales para su	
negocio?	
Hay algún método explícito para proteger los datos, programas y documentación que tienen que ser vitales	
a nuestro, que son vitales para su negocio?	
Disponemos procesos que son perjudiciales o que tienen una vida útil limitada?	
Los datos de procesamiento están protegidos por: Humedad, Alteración de fluidos o alcoholes?	
Existen controles de: Alcaloides que son influenciados dentro como papelería, etc)?	
Existen controles de: Humedad?	
Otros: Existen controles de los productos en gabinetes y productos frágil?	
Mantiene un suministro de pequeños objetos de uso cotidiano, como papel, instrumentos y dinero en su	
establecimiento?	
Todos los objetos de valor son guardados en armarios de metal cerrado con llave?	
Todos los objetos de valor están marcados de una manera?	
Los objetos de valor se retiran de las habitaciones cuando el edificio está desocupado?	

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

INUNDACIONES	Valoración
Nivel (Interruptor)	
Extensión y extensión de inundación para los equipos críticos, los servicios críticos o bienes sensibles? (ej. ¿sólo, algunas áreas?)	
Afectación de Agua	
¿Hay alguna entrada de Agua o derrame de agua en los equipos críticos, los servicios críticos o bienes sensibles?	
¿Es, tampoco de agua, tuberías que atraviesa o cruza por puntos críticos o sensibles?	
¿Hay detectores de humedad dispuestos? cuáles?	
Alarma	
¿Tiene detectores de agua cableados, ¿pero en línea de cualquier equipo eléctrico o sensible? (ej., Computadoras)	
¿Hay una solución impermeable o un pantalla para proteger el equipo dañado de derrames, de agua o con de componente de humedad?	
¿Hay equipos críticos, servicios o bienes sensibles ubicados en el último piso o en el sótano donde se pueda agua de caso de inundación?	
Cable eléctrico	
¿Cable eléctrico dañado con fin de restricción para el paso de agua?	
Fallas de energía	
¿Existe alguna ventanas de fallas, o interacción de las fallas de alimentación o energía?	

INCENDIO	Valoración
Alarma	
¿Existe algún riesgo de incendio en relación contra el edificio? (ej. ¿se encuentra cerca de un tanque con gasolina, almacenamiento de químicos, etc.)	
¿Existe la posibilidad de un aviso(s) bidireccional por su edificio?	
¿Un caso alternativo	
¿Existente tuvieron una forma para protegen el edificio? (ej., una cerca, un muro, un candado)	
Extinguidor	
¿Existe una vía ferrea cerca del edificio?	
¿Existente medios de fallas edificio por accidentes de tren?	
Material inflamable	
¿Hay material en emergencia?	
¿Hay fabricantes, ¿durante su los procedimientos del edificio?	
Agua (Interruptor)	
¿El área encontramos cerca a cuerpo de agua (ej. río, lago, mar)?	
En caso de fallo, ¿Tiene sensores para informar un cambio de humedad o temperatura?	
Mantenimiento	
¿Hay algún material, físico o medio en el mantenido y usado en el edificio?	
¿Hay algún peligro de contaminación, tóxicos del edificio?	
¿Hay algún peligro de contaminación, tóxicos del suelo?	
Seguridad de Datos	
¿Hay algún sistema alterno de terceros en el sitio?	
¿Se encuentra el edificio en una zona donde hay o existieron robos?	
¿Hay antecedentes, o a pesar de los de vandalismo o hostilidad de terceros en la zona? (ej. terrorista, de esos mismos tipos, etc)	

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

EXPLOSIVOS	Valoración
Atentados	
El negocio podría ser victimizado por ataques terroristas?	
Para algún otro negocio o industria vinculo que podría ser victimizado en riesgo de ataques terroristas o de	
Es un edificio de media-alta densidad?	
Tiene un negocio que sufra ataques terroristas?	
La construcción es identificable como un objetivo de ataque?	
El negocio está situado en una zona que podría sufrir ataques terroristas, manifestaciones o disturbios?	
Hay parqueaderos cerca/adyacentes de los bancos u otras del negocio?	
Incendios	
El edificio o bien podría ser objeto de robos?	
Los vecinos tienen sistemas de seguridad, o alarmas contra incendios?	
Se ha identificado en zona de evacuación negra dentro del edificio, donde la gente podría morir en caso de	
Se ha identificado en zona negra de vecindad, a más de 500 metros de distancia?	
Existen un medio sistema de extinción? podría que el pueda utilizar en caso de que el punto contar de extinción	
Entrevistas?	
El área del sector normal tiene una cultura tiene que preparación protección o está no o servicios que cuen	
Incendio de una edificación	

INCLUIDOS	Valoración
Inundación?	
Alguno o todos sus procesos críticos de negocio dependen de la energía eléctrica? (E. equipos no eléctricos o	
servicios)	
Para una sola fuente de energía para el edificio?	
Para una sola fuente de energía para el edificio?	
Existe diferente vecindad de consumidores	
Tiene un mantenimiento de energía y sistema de planta?	
Para una UPS instalada para garantizar la continuidad del negocio?	
En caso de pérdida de energía prolongada y ¿Tiene planes alternos en	
Existe algún tipo de protección contra tormentas?	
Sistema eléctrico, telefónico/Red Interna?	
Tienen sub-centro contactado?	
Los planos electrónicos están en un lugar seguro o en peligro que alguien se interponde su manipuló?	
Suministro de agua	
Alguno o todos sus procesos críticos de negocio dependen de los suministros de agua? (E. refrigerantes	
Los suministros están adecuadamente protegidos?	
Suministro de Gas	
Alguno o todos sus procesos críticos de negocio dependen de los suministros de agua? (E. refrigerantes o	
calderas de vapor)	
Los suministros están adecuadamente protegidos?	
Telecomunicaciones	
Alguno o todos sus procesos críticos de negocio dependen de voces, solicitudes por su conectividad (línea o	
operativa)	
Se encuentran definidas y documentadas todas las funciones y responsabilidades?	

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

COMUNICACIONES	Valoración
Red y Telefonía	
¿Su negocio depende de los sistemas móviles?	
¿Una interferencia de un minuto le hace oír un mensaje de voz?	
¿Tiene teléfonos prioritarios?	
¿Tiene teléfonos de emergencia alternativos?	
¿Cómo sabría si alguien ha interceptado sus llamadas? ¿Son ilegales? ¿Son fáciles? ¿Hay alguien a quien le importe?	
¿Cuánto le costaría? ¿Cuánto le costaría?	
En caso afirmativo, ¿Tiene su contingencia?	
Aplicaciones de Negocio	
¿Alguna o todas las funciones de negocio críticas dependen de una Red de área local (LAN)?	
¿Alguna o todas las funciones de negocio críticas dependen de una Red de área amplia (WAN)?	
¿Su negocio utiliza el correo electrónico de forma considerable o esencial?	
¿Alguna o todas las funciones de negocio críticas dependen de una Red de área de Internet?	
¿Las Redes están protegidas de interferencias?	
¿Tiene cuentas de redundancia de conexión?	
¿Una reacción intervención manual para cambiar las cuentas?	

PROTECCIÓN DE DATOS	Valoración
Información	
¿Existe una política de seguridad de la información?	
¿Existe una persona responsable de la seguridad en todos los sistemas?	
¿Existen los registros que proporcionan información acerca de mantenimiento de sus bienes en el pasado y futuro?	
¿Están los registros actualizados regularmente?	
¿Todos los registros se encuentran adecuadamente protegidos contra el fuego?	
El personal personal se siente satisfecho por el nivel de seguridad?	
¿Existen procedimientos de seguridad para asegurar que el personal nuevo, reposición, visitas son controlados?	
Los registros clasificados están encerrados para salvar a la luz de seguridad?	
¿Son medidas de seguridad en el lugar coinciden con la clasificación de seguridad?	
Personal	
El software propietario es el material de derecho de autor adquirido bajo licencia. ¿Son todo empleados conscientes de esto y de sus responsabilidades?	
¿Existen listas o sobre evaluación del riesgo para verificar si hay cualquiera no observando?	
Hay existencias de esas auditorías?	
¿Existen sistemas rígidos de ello?	
Seguridad física	
¿Seguridad física, de acceso y de control para edificio?	
¿Son suficientes las claves para edificios? ¿Son ellos de seguridad adecuada?	
¿Las cerraduras son cambiadas con frecuencia?	
¿Es limpiador todos los personal en los sistema cuando no están en uso?	
Están los dispositivos de almacenamiento (USB, CD, Encuesta) protegidos y controlados de forma adecuada?	
Es posible la navegación para información sensible en la pantalla?	
La información sensible es transmitida por sonido distributivo, y aplicando ellos indicadores de seguridad?	
¿Los computadores personales están físicamente asegurados contra robo?	
¿La segregación hotel en algún sentido el robo de equipo?	
El seguro sobre la reposición del valor total de los equipos?	

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

PLANES DE CONTINGENCIA	Calificación
Documentos	
Tiene un sitio alterno que podría ser utilizado para albergar todas las funciones críticas del negocio?	
El sitio alterno tiene pruebas recientes?	
El sitio alterno tiene pruebas exitosas?	
El sitio tiene energía eléctrica?	
El sitio tiene personal de vigilia?	
El sitio tiene agua?	
El sitio tiene conexiones de comunicación y red?	
Tiene planes de crisis?	
Planes de Contingencia	
Tiene identificados los procesos de negocios críticos?	
Para todos de ellos tiene un plan bien documentado y probado, efectivo de la empresa?	
Esos planes se han probado en los últimos seis meses?	
Tiene un plan de continuidad de negocio que sea vital a toda la empresa?	
El plan se ha probado en los últimos seis meses?	
Tiene un plan de emergencia?	
El plan se ha probado en los últimos seis meses?	
Tiene un plan de recuperación de desastres de tecnología?	
El plan se ha probado en los últimos seis meses?	
Gestión de Crisis	
Ha tenido incidentes que hayan activado el caso de emergencia?	
Tiene un software especializado para la implantación sistema de alarmas?	
Los recursos y procedimientos del plan serán evaluados como parte de la empresa?	
El plan proveé elementos documentados del retorno de todas las pruebas?	
El plan es regularmente revisado de manera interna que asegura que sea no exista y puede cambiar la	
Los copias de seguridad están asegurados fuera de la compañía?	
Están documentados los procedimientos de como realizar los verificaciones respectivas después de realizarse	
Los Base de Datos?	
Están documentados los procedimientos que detalla todas los procedimientos registrados y alternativas en caso de	
Mantenimiento locales	
Y en resumen, ¿El departamento encargado del Data Center puede recuperar los servicios en otro sitio en la	
Recursos Físicos	
Tiene un inventario detallado de equipos informáticos y de comunicación que no sea los sistemas de cómputo,	
equipo médico, de energía, refrigeración, mejoramientos de espacio, equipo sanitario y una copia de este lista	
mantenida fuera de la compañía?	

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

Clasificación	
Acceso	
Seguridad	
Almacenamiento	
Flexibilidad	
Peligros	
Explosión	
Recursos	
Comunicación	
Protección de datos	
Planes de Contingencia	

Ahora que tiene una apreciación de los riesgos, es necesario desarrollar un plan de acción, para hacerle frente. Seleccione los 4 o 5 más importantes y clasifíquelos por prioridad.

PLAN DE ACCIÓN	PRIORIDAD

8.3. ANALIZAR EL IMPACTO

El BIA constituye la base para elaborar un plan de continuidad de negocio y consiste en describir qué pérdidas potenciales tendrá la organización si alguna de sus actividades de negocio (por ejemplo la facturación o el pago de las nóminas de los empleados) o de los recursos que las soportan (por ejemplo los sistemas informáticos) se paraliza. Este análisis va a permitir que las organizaciones sepan qué recursos van a tener que proveer al plan de recuperación y en qué orden para restablecer y recuperar la operativa después de un desastre.

Dentro del Análisis de Impacto podemos distinguir las siguientes actividades:

ACTIVIDAD 1. Identificar los Procesos Críticos. Se deberá establecer los Procesos de Negocio que se realizan en la compañía y determinar cuáles son los procesos críticos cuya ausencia tendría un impacto alto en la actividad.

A continuación, se presenta una tabla que incluye algunos procesos de negocio de una organización y que podría servir como punto de inicio para identificar y conocer en detalle todas las operaciones de negocio.

Figura 1.03. Procesos de negocio de una organización.

El sistema general propuesto para clasificar el nivel de criticidad de los procesos de negocio es:

- *Criticidad 1: Funciones Críticas – De Misión Crítica.* Son los procesos que deben estar presentes para que se hagan negocios y que si faltan causarían perturbación extrema en la empresa. El requisito de tiempo de recuperación suele ser inmediato.
- *Criticidad 2: Funciones Esenciales – Vital.* Las funciones vitales pueden incluir cosas como la nómina, que a primera vista puede que no sea de misión crítica ya que no son capaces de lograr que el negocio vuelva a funcionar de inmediato, pero que puede ser vital para funcionar más allá de la etapa de recuperación de desastres. El requisito de tiempo de recuperación para este

tipo de procesos suele ser entre el primer y el quinto día después de un incidente.

- *Criticidad 3: Funciones Necesarias – Importante.* Tienen un impacto a más largo plazo, cuando faltan este tipo de funciones y procesos pueden alguna perturbación a la empresa debido a algunas consecuencias legales o financieros, también pueden estar relacionadas con el acceso a través de unidades funcionales y sistemas de negocio. El requisito de tiempo de recuperación suele ser después de la primera semana y antes de un mes.
- *Criticidad 4: Funciones deseables – Menor.* Suelen ser las funciones pequeñas. El requisito de tiempo de recuperación para este tipo de procesos a menudo se mide en semanas o incluso meses.

Obviamente, el Plan de Continuidad del Negocio centrará más tiempo y recursos en el análisis de las funciones críticas.

ACTIVIDAD 2. Análisis de Recursos. Durante esta actividad se deberá recoger el inventario de los recursos que soportan los procesos de la compañía, a fin de identificar aquellos que dan soporte directo a los servicios críticos. Los tipos de recursos que se deben analizar son: cada uno de los elementos hardware que soportan los sistemas de información de la compañía, las aplicaciones de gestión que son utilizadas en la empresa, el personal involucrado en los mismos, muebles y alojamiento, papelería, métodos y servicios de comunicación, equipos especiales y necesidades específicas de TI. Además se deberá clasificar categoría de criticidad de los recursos, así:

- *Categoría 1.* La organización/departamento no puede funcionar sin el recurso.

- *Categoría 2.* La organización/departamento funciona parcialmente sin el recurso.
- *Categoría 3.* La organización/departamento puede funcionar sin el recurso.

ACTIVIDAD 3. Determinar las interdependencias de recursos. Son las relaciones cliente/servicio que soportan las operaciones comerciales normales. Se deberán listar todos los insumos que son críticos para el éxito del área o proceso de negocio y quienes son los proveedores del servicio o proceso. Algunos ejemplos de recursos críticos pueden ser: las redes de comunicaciones en organizaciones que dependen de las comunicaciones internas y externas para funcionar adecuadamente, los sistemas de alimentación energética en aquellas compañías que requieren de suministro eléctrico para fabricar sus bienes, el conocimiento del fundador o gerente de la empresa, el cual es el único que dispone de la experiencia y entendimiento detallado de sus actividades de negocio, el listado de clientes y contactos comerciales disponible únicamente en soporte papel.

ACTIVIDAD 4. Determinar el impacto. La valoración de pérdidas no es una cuestión sencilla, ya que pueden concurrir aspectos intangibles, tales como la imagen de la organización ante sus clientes. Algunos criterios que pueden ayudar a valorar las eventuales pérdidas pueden ser: costo de horas de trabajo perdidas, al no poder usar las aplicaciones que no tengan alternativa manual o cuyo tratamiento manual suponga una pérdida de eficiencia importante, ingresos dejados de percibir, penalizaciones por incumplimiento de contratos con clientes, sanciones administrativas por incumplimiento de leyes debido a la falta de control en situación de desastre, gastos financieros,

Figura 19. Tipos de Impac to

ACTIVIDAD 5. Determinar el Periodo Máximo de Interrupción. A medida que pasan los días y las actividades siguen interrumpidas, las pérdidas suelen ir creciendo linealmente, sin embargo, a partir de un momento que denominaremos ***Tiempo Máximo de Interrupción***, las pérdidas sufren un aumento significativo, afectarían de forma grave a la compañía y las funciones no podrían ser reasumidas.

Existen dos parámetros muy específicos que están estrechamente relacionados con la recuperación: ***Tiempo de Recuperación Objetivo (RTO)*** y ***Punto de Recuperación Objetivo (RPO)***.

El ***RTO*** establece la urgencia que las diferentes unidades de negocio precisan para volver a su funcionamiento habitual. Por tanto, determina los plazos en los que deben volver a funcionar con normalidad. Estos pueden establecerse en períodos de tiempo en función de la criticidad de los procesos y pueden ser cuestión de horas o semanas en aquellos procesos prescindibles. Por tanto, se

trata de identificar el orden en que hay que tratar de reconstruir la actividad, recuperando antes aquellos procesos cuya paralización suponen un mayor impacto para la organización. En una situación de crisis siempre hay recursos limitados y es necesario elegir qué hacer primero atendiendo a un criterio de negocio.

El ***RPO*** se refiere al punto más reciente en el tiempo en el que los sistemas pueden ser recuperados, reflejando por tanto cuánta es la cantidad de información que una organización puede permitirse perder sin que le afecte negativamente. Por tanto, el RPO determina la periodicidad con la que deben salvaguardarse los datos para todos aquellos procesos de negocio.

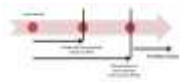


Figura 16. Tiempos de #recuperación

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

HERRAMIENTA DE ANALISIS DE IMPACTO

Instrucciones
Previo diligenciar de esta análisis, la empresa ya conocerá conformada por cada una de procesos de negocio, actividades inter relacionadas y en cuanto medida interdependientes.
Se debera diligenciar completo este documento para cada una de los procesos de negocios.
Las técnicas sugeridas en el presente documento se ofrecen como un conjunto de directrices, que pueden no ser tenidas me completas. Su eficacia dependerá de la capacidad del usuario para evaluar e integrarlas en su entorno operativo propio.
Se recomienda que mínimo 3 personas por cada proceso de negocio este involucrados en este análisis.
Cualquier información introducida en este documento es confidencial y debe ser tratada como tal.
ANALISIS DE RECURSOS: expida todos los recursos necesarios para el proceso de negocio.
IN TERDEPENDENCIAS CRITICAS: tiene todos los insumos necesarios para el éxito del área o proceso de negocio y quienes son los proveedores. Ej. redes de comunicaciones, alimentación energética
TIEMPOS CRITICO DE OPERACIÓN: mencionar las ocasiones en que hay plazos o fechas de cumplimiento específicas. Ej. Pago de impuestos por ley, liquidación de nómina o fin de año.
IMPACTO: expida los problemas o dificultades de tipo operativo que pueden presentarse y los costos financieros y consecuencias intangibles debido a la degradación del proceso.

Nivel de Criticidad del Proceso en Negocio
1 - Funciones Críticas – De Misión Crítica
2 - Funciones Esenciales – vital
3 - Funciones Necesarias – importante
4 - Funciones deseables – Menor

Frecuencia de Criticidad de los Procesos
1 - La organización/departamento no puede funcionar sin el recurso.
2 - La organización/departamento funciona parcialmente sin el recurso.
3 - La organización/departamento puede funcionar sin el recurso.

PROCESO DE NEGOCIO	
Nombre	
Responsable	
Analistas Análisis	Fecha
Área	
Breve descripción	
Procesos	Nivel Máximo de Interrupción (MTO)

INVENTARIO DE RECURSOS				
Proceso (Actividades de Negocio)	Descripción	Categoría	Cantidad	Alternativa / Costo
Necesidades específicas de TI				
Comunicaciones				
Documentación				
Procesos Manuales				
Personal				
Objetivos y Alcances				
Soporte				
Equipo Especial				

Sistemas que soportan el Proceso				
Nombre	Descripción	Categoría	Nivel de Importancia	Prioridad de Recuperación

Hardware que soportan el Proceso				
Tipo	Modelo y Capacidad	Cant.	Nivel Normal	Nivel Crítico

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

INTERDEPENDENCIAS CRITICAS				
Servicio / Proceso Crítico	Proveedor Regular	Ubicación del Proveedor	Proveedor Alternativo	Ubicación de Proveedores

TIEMPOS CRÍTICOS DE OPERACIÓN		
Función o Actividad Afectada	Duración	Impacto en el Negocio
	Hrs, Días, Semanas	

IMPACTO		
Afectación Organizacional	Clientes Perjudicados	Afectación Económica

8.4. DETERMINAR LA ESTRATEGIA DE RECUPERACIÓN

Las estrategias de recuperación son procesos focalizados en cómo recatar a la organización en caso de que un desastre se presente. Son mecanismos relacionados con la implantación de procedimientos de respuesta ante emergencias y la posibilidad de activar los mecanismos preventivos que ya han sido implantados. En esta fase se seleccionarán los métodos operativos alternativos que se van a utilizar en el caso de que ocurra un incidente que provoque una interrupción en la organización. El método seleccionado deberá garantizar la reanuación de los procesos afectados en los tiempos determinados por el Análisis de Impacto.

La organización debe tener en cuenta los posibles daños potenciales a la hora de revisar y seleccionar las diferentes soluciones o alternativas de recuperación de sus actividades críticas, considerando adicionalmente los siguientes factores:

- El costo económico asociado a la implantación de la estrategia de recuperación, la cual suele constituir uno de los mayores inconvenientes a la hora de adquirir una solución de recuperación.
- Los beneficios que proporciona la estrategia.
- El Tiempo Máximo Permitido de Interrupción (MTD) de la actividad crítica.
- El Tiempo de Recuperación Objetivo (RTO).
- La pérdida máxima de información que una empresa se puede permitir (RPO).

Una vez analizadas y seleccionadas las estrategias de recuperación que serán empleadas como respaldo en caso de interrupción de las actividades críticas de

negocio, es necesario plasmar todas las soluciones y pasos a abordar en un plan (entendido como un conjunto de procedimientos, funciones y actividades que permitirá el restablecimiento de las citadas actividades en unos plazos razonables).

Considerando únicamente las instalaciones y puestos de trabajo de la empresa como recurso crítico, la siguiente tabla propone diferentes estrategias de recuperación dependiendo del Tiempo de Recuperación Objetivo (RTO).

Figura 1917. Resumen de las estrategias de recuperación con respecto al tiempo de recuperación.
Fuente: Business Continuity Institute

La siguiente tabla propone diferentes estrategias de recuperación para distintos recursos críticos de la organización.

Figura 167. Ejemplos de estrategias de recuperación

8.5. DESARROLLAR E IMPLEMENTAR EL PLAN

Una vez que se ha seleccionado la estrategia de respaldo hay que desarrollarla e implantarla dentro de la compañía. En esta fase se desarrollan los procedimientos y planes de actuación para las distintas áreas y equipos, y se organizan los equipos que intervienen en cada fase del Plan. Así los esfuerzos pasan de una fase de planificación a una fase de acción e implementación.

Todo plan de continuidad de negocio fracasará si previamente no se han dimensionado y provisionado los medios y recursos necesarios que permitan su ejecución. De acuerdo a las estrategias de recuperación diseñadas con anterioridad, las organizaciones deberán dotarse de los recursos indispensables para el desarrollo efectivo de la respuesta, algunos de estos recursos son: transporte, medios de almacenamiento, servidores, PC's, dispositivos móviles y de comunicación, recurso humano, información crítica redundante y necesaria para el desarrollo de las actividades de negocio.

También es importante que el plan de continuidad de negocio esté disponible para las personas que participan en el mismo en diferentes formatos (electrónico y en papel) y deben mantenerse copias en diferentes ubicaciones (al menos una de estas debe estar alejada de las oficinas o domicilios en las se desarrollan las actividades críticas de la organización.

Dentro del Desarrollo del Plan de Continuidad del Negocio podemos distinguir las siguientes actividades:

ACTIVIDAD 1. Definir y organizar los equipos. Los equipos de emergencia están formados por el personal clave necesario en la activación y desarrollo del Plan de Continuidad. Cada equipo tiene unas funciones y procedimientos que

tendrán que desarrollar en las distintas fases del Plan. Es posible destacar funciones clave que serán llevadas a cabo por los responsables (personas o equipos, dependiendo del tamaño y de los recursos de la empresa) de la activación y ejecución del plan de continuidad de negocio:

- *Respuesta a incidentes:* responsables de analizar y acotar el impacto que una incidencia puede provocar en la organización de forma que no se tenga que recurrir a la activación del plan de continuidad de negocio.
- *Comité de crisis:* encargado de activar el plan de continuidad de negocio y dirigir las acciones durante la contingencia. Este Comité debe tomar las decisiones "clave" durante los incidentes, además de hacer de enlace con la dirección de la compañía, manteniéndoles informados de la situación regularmente. Las principales tareas y responsabilidades de este comité son: Análisis de la situación, Decisión de activar o no el Plan de Continuidad, Iniciar el proceso de notificación a los empleados a través de los diferentes responsables, Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación.
- *Servicios civiles de emergencia* necesariamente localizables en caso de catástrofe (como por ejemplo los bomberos) que generalmente constituyen la primera figura de respuesta.
- *Logística* responsable de reunir todos los medios (lugar alternativo de trabajo, material, herramientas, transporte de material y personas, comida, reservas de hotel, etc.) necesarios para contribuir a la reactivación de la actividad. Este equipo debe trabajar conjuntamente con los demás, para asegurar que todas las necesidades logísticas sean cubiertas.

- *Recuperación*: asume la puesta en servicio de la infraestructura tecnológica (sistemas, servidores, aplicaciones, líneas de comunicación y cualquier otro elemento necesario para la restauración de un servicio).
- *Relaciones públicas*: Se trata de canalizar la información que se realiza al exterior en un solo punto para que los datos sean referidos desde una sola fuente. Responsable de las comunicaciones con clientes, accionistas, elaboración de comunicados para la prensa, medios de comunicación, etc.
- *Unidades de Negocio*: Estos equipos estarán formados por las personas que trabajan con las aplicaciones críticas, y serán los encargados de diseñar y realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas y comenzar a funcionar.

El personal asignado a cada uno de los equipos puede variar dependiendo del tamaño de la organización y de la estrategia de recuperación seleccionada. Una persona puede pertenecer a más de un equipo, siempre y cuando no existan incompatibilidades en las tareas a realizar. Una vez que se han definido las figuras o equipos, así como las funciones a desempeñar por los mismos, la empresa debe desarrollar los planes o procedimientos de actuación a seguir.

ACTIVIDAD 2. Desarrollar los procedimientos. Estos procedimientos, recogen el conocimiento necesario para la activación y ejecución del plan de continuidad de negocio, ya que reducen el tiempo invertido en la toma de decisiones críticas y acotan los momentos de incertidumbre y el tiempo de reacción. Deben ser concisos, factibles y accesibles a todos aquellos miembros que tienen algún tipo de responsabilidad de actuación dentro del plan.

RESPUESTA A INCIDENTES. Cualquier incidente que tenga lugar en la organización y que interrumpa sus actividades críticas debe contar con un *Plan rápido de respuesta* que permita confirmar el tipo de incidente y su criticidad, tomar el control de la situación problemática generada por el incidente y acotar o limitar el impacto que dicho incidente pueda provocar.

A continuación se muestra la secuencia de tareas a realizar en caso de que una empresa detecte la paralización de sus actividades críticas.

Figura 19B. Secuencia de tareas en caso de paralización de la actividad.

PROCEDIMIENTO DE RECUPERACIÓN. Tiene como objetivo recuperar en el menor tiempo posible las actividades críticas de una organización que se han visto interrumpidas por un desastre. Debe contener la siguiente secuencia de procedimientos:

- *Procedimiento de notificación del desastre.* Como parte del Plan de Continuidad se debe establecer un programa de concientización, en el que se informe al personal cómo debe actuar ante estos casos y a quién comunicar lo ocurrido.

- *Procedimiento de lanzamiento del Plan.* Una vez que un miembro del Comité de Crisis es contactado e informado del incidente, procederá a evaluar la situación con la recopilación de la mayor información posible. El Comité se reunirá en un lugar acordado previamente y evaluará la situación. Este Comité deberá informará a los responsables de los distintos equipos de lo ocurrido y de la situación en ese momento para que permanezcan en situación de espera, hasta que se tomen la decisión de disparar el Plan o iniciar otro tipo de estrategia.

- *Procedimiento de notificación de la puesta en marcha del Plan a los equipos implicados.* Una vez que el Comité de Crisis ha decidido poner en marcha el Plan de Recuperación, debe de iniciarse el árbol de llamadas para comunicar a los Responsables y componentes de cada equipo la situación de inicio de las actividades del Plan para comenzar los procedimientos de actuación de cada uno de ellos.

- *Procedimiento de concentración y traslado de equipos.* Dependiendo de la solución final que se decida como estrategia de respaldo, este procedimiento puede variar. Una vez avisados los equipos deberán acudir al centro de reunión. En el caso de que la emergencia se declare en horas de trabajo, se tomará como punto de encuentro los lugares designados en el Plan de Emergencia. Si el incidente ocurre fuera del horario de trabajo, el lugar de reunión será el designado como centro de respaldo, o cualquier otro designado por el Comité de Crisis. También que realizar una importante labor de coordinación para el traslado de todo el material

necesario para poner en marcha el centro de recuperación (cintas de backup, material de oficina, documentación)

- *Procedimiento de puesta en marcha del centro de recuperación*. Teniendo los distintos equipos y elementos necesarios disponibles para comenzar la recuperación, hay que poner en funcionamiento este centro, implantando la infraestructura necesaria, tanto de software como de comunicaciones, etc.

- *Procedimientos de restauración*. Se refiere a las acciones que se llevan a cabo para restaurar los datos y sistemas críticos. Suele precisar los mayores esfuerzos e intervenciones para cumplir con los plazos fijados.

- *Procedimientos de soporte y gestión*. Una vez restaurados los sistemas hay que comprobar su funcionamiento, realizar un mantenimiento sobre los mismos y protegerlos, de manera que se reanude el negocio con las máximas garantías de éxito. Los integrantes del equipo de unidades de negocio serán los encargados de comprobar y verificar el correcto funcionamiento de los procesos.

A continuación se muestran algunos ejemplos característicos de procedimientos de recuperación ante la supuesta indisponibilidad de recursos críticos de la empresa.

Figura 1420. Procedimiento de recuperación caracteristicas

PROCEDIMIENTO DE VUELTA A LA NORMALIDAD. Una vez solucionada la contingencia y recuperadas las actividades críticas de la organización, deben establecerse los mecanismos necesarios para recuperar totalmente el funcionamiento normal de las actividades, para ello se deberá realizar un análisis o valoración detallada de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad que incluye acciones como compra de nuevos equipos, muebles, material, etc.

Finalmente, cada equipo deberá realizar un informe de las acciones llevadas a cabo y sobre el cumplimiento de los objetivos del Plan de Continuidad, los tiempos empleados y dificultades con las que se encontraron. Toda esta información servirá para valorar si el Plan ha funcionado según lo planeado, conocer los posibles fallos, y así tenerlos en cuenta para la adecuación del mismo.

PLANTILLA DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

I. [illegible]

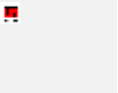
[illegible]

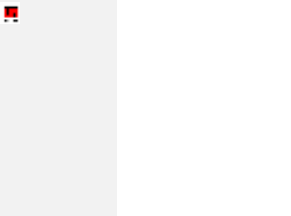
[illegible]

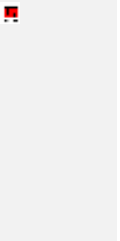
[illegible]

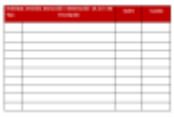
[illegible]

[illegible]









8.6. MANTENER EL PLAN

El hecho de elaborar y documentar planes de continuidad de negocio y procedimientos de recuperación en caso de paralización de las operaciones no garantiza el éxito a la hora de enfrentarse a un desastre. Una parte importante del Plan de Continuidad, es conocer que realmente funciona y es efectivo. Para ello se define la estrategia de pruebas y se realiza la prueba del Plan, para almarlo según los resultados, además, en esta última fase se definirán los procedimientos de mantenimiento del Plan.

Dentro del Mantenimiento del Plan de Continuidad del Negocio podemos distinguir las siguientes actividades:

ACTIVIDAD 1. Distribución y Formación. Una emergencia no es el mejor momento para estudiar documentación y manuales, por lo tanto gran parte del esfuerzo debe destinarse a la formación del personal para que pueda asimilar su papel en momentos de crisis y conocer perfectamente las tareas que se espera desempeñe. Incluso cabe la posibilidad de extender estos programas de formación a proveedores o tercerss con las que la organización mantiene relaciones comerciales.

Todas las partes interesadas recibirán sesiones de entrenamiento regulares acerca de los procedimientos y roles a ser seguidos en caso de un incidente o desastre. Se deben utilizar diversos medios para la impartición efectiva de la información, como por ejemplo, la publicación de mensajes y contenidos relacionados con la continuidad de negocio en la Intranet o plataformas online semejantes. Se llevará un registro de cada sesión de capacitación que incluya: Planillas de Asistencia a Entrenamiento, Número de personas que han asistido a

entrenamiento, Porcentaje de personas que han asistido.

Como el plan contiene información sensitiva para la compañía, debe ser distribuido solo a las personas autorizadas, deber ser dividido en secciones que se entregarán a cada persona según sus funciones dentro del Plan (se entregará solamente lo que "necesita saber").

ACTIVIDAD 2. Ejecución de Pruebas. Desarrollado e implantado el plan de continuidad de negocio, es recomendable que sea probado periódicamente. La organización debe planificar pruebas, su duración y alcance, los participantes (incluidos proveedores de servicios), los elementos del plan que serán evaluados (personas, comunicaciones, sistemas, procedimientos) y la secuencia de pasos a emprender durante su ejecución. Las pruebas deben simular situaciones cercanas a la realidad y deben ser planificadas de forma que la exposición de las actividades de la organización ante los riesgos sea mínima. Aunque sería lo ideal, las compañías que deciden realizar tales pruebas no pueden permitirse el lujo de detener completamente su producción, por lo que las pruebas deben realizarse en áreas y momentos específicos que no castiguen la entrega de sus productos y servicios. Los tipos de pruebas a realizar son:

Figura 21. Tipos de Pruebas del Plan de Continuidad del Negocio

ACTIVIDAD 3. Actualización. Los planes de continuidad de negocio deben ser mantenidos a través de un ciclo de mejora continua. Cualquier cambio a nivel estratégico, operacional o técnico puede impactar en el negocio y por tanto en el plan de continuidad. Por lo cual, la empresa deberá iniciar un proceso para mantener al día la capacidad, eficacia e idoneidad del plan de continuidad de negocio y de esta forma, se pueda disponer de ciertas garantías sobre la efectividad del plan. Algunas propuestas en ese sentido son:

- Revisión periódica en busca de cambios en la estructura de la organización, y en los productos/servicios que desarrolla, los cuales pueden tener consecuencias en el Plan de Continuidad del Negocio (política, BIA, procedimientos de recuperación, etc.) y confirmar que estos cambios han sido aplicados.
- Adecuación de los planes de continuidad de negocio a requerimientos de socios, clientes, accionistas u otro tipo de requerimientos normativos.

- Revisión de los resultados de las pruebas realizadas y de que las mejoras identificadas en las mismas han sido aplicadas.
- Auditorías internas o externas de todos y cada uno de los componentes del Plan de Continuidad del Negocio.

HERRAMIENTA PARA EL REGISTRO E INFORME DE PRUEBAS

INFORME DE PRUEBA

Prueba de Recuperación

CASO DE ESTUDIO

ANTECEDENTES

La Asociación Mutual Barrios Unidos de Quibdó E.P.S. es una empresa solidaria integrante del Sistema de Seguridad Social en Salud, la cual ha desarrollado una Plataforma Estratégica que le permite adecuarse funcional y estructuralmente a los cambios internos y exigidos por el entorno. Actualmente cuenta con 700.000 afiliados y 400 empleados, repartidos en 9 sedes administrativas ubicadas en Barranquilla, Cartagena, Valledupar, Sincelejo, Santa Marta, Riohacha, Quibdó, Maganguè y Cartago, además de varios centros de atención al público a nivel nacional. Tiene una estructura de departamentos, así:

La oficina principal se encuentra localizada en Barranquilla, en una zona comercial sobre una avenida que diariamente moviliza automóviles y vehículos particulares, y en el segundo piso de un edificio de 5 pisos compartido con varias empresas.

El edificio recibe la energía eléctrica de una compañía local, cuenta con una planta con una capacidad estimada de 10 horas de operación, por lo cual las fluctuaciones de energía eléctrica no son una preocupación inmediata ni afecta a los clientes o usuarios internos. La empresa cuenta con un sistema electrónico de seguridad y cada empleado tiene acceso a las diferentes áreas de acuerdo a sus necesidades. No se cuenta con un sistema electrónico de detección y extinción de incendios, pero existen extinguidores de fuego ubicados estratégicamente por todo el edificio.

El departamento de sistemas depende de la Dirección Administrativa, se encuentra formado por 12 empleados que se encargan de la gestión de todo lo relacionado con comunicaciones, software, hardware, bases de datos. Estos empleados tienen acceso permanente al centro de datos. El departamento y su centro de datos se encuentran ubicados en Barranquilla.

Los 6 servidores principales están altamente integrados en un Blade formado por 12 procesadores con múltiples subsistemas de discos. El centro de datos es enfriado por agua y el sistema de aire acondicionado está ubicado en el centro de cómputo. Los servidores soportan alrededor de 5.000 operaciones batch por mes, adicional al tráfico tanto interno como externo desde y hacia los clientes.

La operación diaria de la compañía está automatizada y depende del centro de datos, el sistema de comunicación de voz y las redes LAN y WAN. Cuenta con 16 canales telefónicos de voz de entrada donde las llamadas se distribuyen a través de una planta telefónica. Además cuenta canales de datos redundantes con

diferente proveedor. La compañía usa el correo electrónico fuertemente como medio de comunicación interno.

El Departamento de Recursos Humanos y su jefe reportan a la Dirección Administrativa, se encarga de la contratación de personal, contabilización de novedades, liquidación de nómina y seguridad social. Hay alrededor de 10 personas en este departamento. Se espera que este departamento esté completamente funcional y operativo máximo 20 días después de un desastre mayor. Ninguno de los empleados tiene acceso al centro de datos y sólo se les permite el acceso con una autorización previa.

La Dirección de Aseguramiento es responsable de todo el contacto, afiliaciones con los clientes y seguimiento a los servicios. El personal está organizado funcionalmente y son aproximadamente 50 personas. Cada uno de los empleados de esta área debe tener un teléfono y un portátil para acceder a la información, estado del trabajo y correo electrónico corporativo. Se espera que este departamento esté completamente funcional y operativo máximo 5 días después de un desastre mayor. Ninguno de los empleados tiene acceso al centro de datos y sólo se les permite el acceso con una autorización previa.

La Dirección de Financiera es de las actividades diarias de contabilidad, cartera, facturación, tesorería. El personal está organizado funcionalmente y son aproximadamente 25 personas. Cada uno de los empleados de esta área debe tener computador para acceder a la información en el sistema financiero y correo electrónico corporativo. Se espera que este departamento esté completamente funcional y operativo máximo 5 días después de un desastre mayor. Ninguno de los empleados tiene acceso al centro de datos y sólo se les permite el acceso con una autorización previa.

El rápido desarrollo y expansión de esta compañía ha resultado en un crecimiento

tecnológico importante en los procesos de soporte, tales como facturación, nómina, atención al cliente, etc. Sin embargo, las medidas de seguridad no han acompañado de igual forma a este crecimiento. A continuación, se describe brevemente cuál es la situación actual en cuanto a seguridad de la compañía: No existe una política de seguridad en la compañía, sólo hay antivirus en algunos equipos, se realizan copias de seguridad de la información pero no se encuentran resguardadas fuera de la compañía, existe control de acceso a los equipos pero los usuarios comparten contraseñas o no bloquean la sesión.

Como parte de los proyectos a llevar a cabo durante el año 2011, el Director de Sistemas ha propuesto la realización de un Plan de Continuidad de Negocio, para configurar una estrategia de recuperación ante cualquier evento grave que haga peligrar el negocio de la empresa. Para desarrollar este Plan, ha encargado a un responsable en el departamento de sistemas de realizar un inventario de los procesos críticos de la compañía, estableciendo los tiempos de recuperación de los mismos, antes de incurrir en pérdidas graves. Para ello, se han entrevistado con los responsables de los procesos obteniendo la siguiente información:

ANALISIS DE IMPACTO

Para el ejemplo sólo se tomará un proceso de muestra (Gestión de Nómina)

Ficha de la Entrevista			
Gestión	Gestión de Nóminas		
Responsable	Gestor de Talento Humano		
Fecha de Análisis	Enero de 2012	Criticidad	Moderada
Breve descripción	Gestión de pagos de nóminas (MOM, empleados, cálculo de parafiscales mensuales, retenciones y pagos)		
Alternativa	No implantar	Tiempo Máximo de Interrupción (MAO)	15 - 22 días

Aunque el proceso de Gestión de Nómina es importante, la compañía puede esperar semanas a que se restablezca y crear procedimientos alternativos como repetir el último pago de nómina a los trabajadores y realizar las compensaciones

correspondientes, cuando estén disponibles los sistemas nuevamente.

Anexo02 de MEGRUR				
Impacto del Proceso de Negocio	Descripción	Categoría	Cantidad	Ubicación / Zona
Dependencias Específicas de TI	Impresora de matriz de puntos	2	1	Principal
	Fax	2	1	Principal
Comunicaciones	Red LAN	3	1	Principal
Documentación				
Procesos Manuales	Cuadernos	1	1	Principal y Negocio
	Registro Biológicos Diarios	1	1	Principal
Personal	Técnico - Mario Abel Hernán		1	Principal
	Técnico - Octavio Hernandez	1	1	Principal
	Técnico Contratista	2	1	Principal
Documentos y Medios	Planos	1	1	
	Manuales	1	1	
	Archivos	1	1	
Seguridad	Llaves de puerta (resguardadas con seguri	1	1	Principal
Equipo Especial				

Sistemas que soportan el Proceso				
Nombre	Descripción	Categoría	Modelo de Operación	Ubicación / Zona
(Vivir Isotermo	Sistema Externo de Monitoreo de Temperatura de Heladeras	1	Centralizado	Abel Cuenca

Software que soporta el Proceso				
Nombre	Descripción / Especificación	Categoría	Modelo de Operación	Ubicación / Zona
Servidor	IBM BladeCenter S - 1 Gabinete - Blade HS22 con 2 procesador Quad Core Xeon E5310 1.60 GHz, 8 MB L2 Cache, 1.066 FSB en Rack 2 (10.1.0.0/24 en RAS1)	2	Abel	Principal
PCs	Dell Optiplex 760 - Intel Core 2 New 3MB 2.4 GHz - 4Gb RAM - 320GB DD	2	Dell	Principal
TOKEN	TOKEN TRANSACCIONES BANCARIAS	1	Nuevo Gaucamento	Principal

INTERRUPCIONES CRÍTICAS				
Servicio / Proceso Crítico	Proveedor Regular	Situación del Proveedor	Proveedor Alternativo	Distribución Geográfica
ANDEX / CONEXIA ACTIVO	TELEFONICA	Calle 76 num 53	UNIFIRM	Duplicidad en Centros de Datos

TIEMPOS CRÍTICOS DE OPERACIÓN		
Función Individual Afectada	Duración Máxima Tolerable	Impacto para Negocio
Pago de Nómina	Ultimo Semana del Mes	Regulatorio
Pago de Nómina	Ultimo Semana del Mes	Económico

IMPACTO		
Efectuados/Operativos	Costos Tangibles	Costos Intangibles
Error en la Dispersión de salarios y prestaciones sociales.	Posibles Financiera por sanciones internas al incumplimiento	
No pago a la seguridad social	Posibles financieras por sanciones internas al incumplimiento.	Posibles disrupción anuncios, inconvenientes, y diversos.

ANALISIS DE RIESGOS

Tomando como ejemplo el inventario de los procesos descritos en el análisis de impacto y las premisas descritas en la presentación de la compañía, se elabora el siguiente análisis:

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

INCENDIO	Valoración
Nombre:	
¿La alarma de incendio del edificio está instalada directamente al servicio local de bomberos?	0
¿Tiene extintores de fuerte rociadores?	0
¿Los detectores de humo pueden funcionar si hay un fallo de luz?	0
¿Hay suficientes salidas de fácil acceso?	0
¿Hay un sistema de alarma de incendios en el edificio?	0
¿Hay algún mecanismo de alerta a los ocupantes del edificio?	0
¿Hay algún documento donde del edificio (Ej. plano o croquis) disponible?	0
¿Hay un historial de incendios frecuentes?	0
¿Ha habido en ocasiones de evacuación de incendios durante los últimos seis meses?	0
¿Se tienen en cuenta las recomendaciones de la aseguradora de su sitio de tendencia local?	0
¿Se ve en desde el personal durante la construcción de extintores?	0
¿Conocen todos los equipos de fuego cuando el edificio está desocupado?	0
¿Existe una persona para la prevención y control de incendios que responsable en cada piso?	0
PLAN DE CONTINUIDAD DEL NEGOCIO	
¿Hay edificio una persona de peligro de incendio (Ej. daño que no sea posible para cubrir o permanecer en edificio)?	0
¿Se ha definido el plan integral con los objetivos de su empresa?	
¿Es un plan de excelencia	0
¿Hay un comité de excelencia cada 30 días / mensualmente?	0

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

SEGURIDAD	Valoración
Organizar	
La seguridad general del personal o el encanto protegido ?	1
La seguridad de las definición de encanto protegido ?	1
Mala seguridad en la casa de emergencia?	1
Mala seguridad en la casa de emergencia?	1
El personal trabajo en el encanto la seguridad y el encanto protegido?	1
Está permitido el acceso al personal de seguridad a sus oficinas?	1
Es animado el Bien Center de a través de la calles y partirlo de encanto?	1
Las Tarjetas de acceso son usadas por todos los empleados para la seguridad?	1
Existe en el proceso de renovación llenos que recoge la Vida de Alquiler y se Desarrolla a la compañía Como zona, las áreas de identificación a acceso, etc?	1
Existe un procedimiento de Seguridad Física y Para visita de ingreso?	1
Existe un sistema de alarmas?	1
En caso afirmativo, ¿Está conectado directamente a los servicios de emergencia?	1
Existe un procedimiento de alerta con ordenes a la vista a mano cercana?	1
SEGURO	
¿Está asegurado todos los bienes?	1
Que oficinas están cubiertas por la noche?	1
Que oficinas están cubiertas por el día?	1
Son conocidos el alcance y el valor de la reposición? Bien de distributivo que implican que algún puede ser asegurado durante la vida útil de reclamación?	1
Para cubrirse de seguridad Física del edificio?	1
Para cubrirse de seguridad dentro de las instalaciones?	1
Cuenta con personal capacitado con medidas para primeros auxilios?	1
Y en el, ¿ha seguido las recomendaciones?	1

ALMACENAMIENTO	Valoración
Como son todos los seguros que usted utiliza? Existen los bienes y encargados a mantenerlos?	1
Tiene copias de seguridad de los manuales de instrucciones y de mantenimiento?	1
Existen procedimientos, programas y documentación donde indiquen con los procesos que son vitales para su Oficina?	1
Existe algún medio especial para proteger los datos, programas y documentación de que tienen que ser con respecto del con miras para su reinicio?	1
Almacenar productos que con perecederos o que tienen una vida útil limitada?	1
Este área de almacenamiento tiene protección de? Humedad, Alta fuente de incendio o de fuego?	1
Escribe cuidadosamente de productos que son influencias Sobre como expedirlo su uso?	1
Escribe cuidadosamente de productos que son influencias Sobre como expedirlo su uso?	1
Como Trabaja el personal en el almacenamiento y el uso de Gas?	1
Existe en un inventario de pequeños objetos de valor tales como joyas, instrumentos y dinero en los establecimientos?	1
Todas las objetos de valor son guardados en armarios de metal cerrado con llave?	1
Todas las objetos de valor están bajo llave de cierre diario?	1
Los objetos de valor se retiran de los instalaciones durante el tiempo mas razonable?	1

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

INUNDACIONES	Valoración
Nivel (Intensidad)	
¿Existe una estimación del inundación para los equipos críticos, los servicios vitales o bienes valiosos? (p. ej., 100 años, 500 años)	0
Daños	
¿Hay algún enemigo de flujo o derrame de agua en los equipos críticos, los servicios vitales o bienes valiosos?	0
(1). tamaño de agua, ¿alcanza por encima o cubre por completo alguno el equipo	0
Hay diferentes de humedad debajo del suelo?	0
¿Tiene electrónico de agua ubicados, justo encima, de cualquier equipo eléctrico sensible? (1). Computadoras)	0
¿Hay una sistema impermeable disponible para protegen el equipo después de diferentes de agua o acc de temperatura de inundar?	0
¿Hay equipos en fluvio, servicios vitales o bienes activos ubicados en el último diseño o encima agua en caso de inundación? (1). Computadoras)	0
Cada cuanto ¿Afecta cortar el suministro principal de agua?	0
Costo de daños	0
¿Existe algún enemigos de fallas o corrosión en las tuberías de alcantarillado o drenaje?	0

FELUDOS	Valoración
Activos	
¿Existe algún riesgo de choque de un vehículo contra el edificio? (1). Le encuentra cerca del cerrilleros con	0
¿Existe la posibilidad de un peligro meteorológico?	0
¿Existe la posibilidad de un peligro meteorológico en vehículo?	0
En caso afirmativo, ¿Se puede blanear una barrera para protegar el edificio? (2). una valla, un muro, un jardín	0
Personas	
¿Existe una ola de frio cerca del edificio?	0
¿Existe el riesgo de edificio afectar a un accidente de tránsito?	0
Personas	
Hay cerca de un aeropuerto?	0
Hay peligro a fluctuaciones, relacionado en la geomorfología del edificio?	0
Del desarrollo	0
El uno posible cesado está a cerca de interrumpiendo?	0
Existen algunos riesgos cercanos que no afectarán el servicio de movilidad o temperatura?	0
Activos	
Hay algún material dentro o explosivo inflamando y cuelo en el edificio?	0
Hay algún material dentro o explosivo inflamando cerca del edificio?	0
Hay algún peligro de contaminación cerca a los del suelo?	0
Personas y del Suelo	0
Hay algún antecedente de terremoto en el área?	0
El terremoto en el edificio de una zona donde hay o volcánico activo ?	0
Hay cerca de la proximidad de mantenimiento o fundamentos de tierra en la área? (2). corrientes de agua cuales cerca, etc	0

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

EXPLOSIONES	Valoración
Terrorismo	
El negocio podría ser amenazado por ataques terroristas?	0
Hay algún otro negocio o industria cercana que podría ser vulnerable en riesgo de ataques terroristas o de explosiones?	0
Es probable que exista multa considerable?	0
Tiene su negocio que sufrir ataques terroristas?	0
La comunicación es identificada como un objetivo de ataque?	0
El negocio está situado en una zona que podría sufrir ataques terroristas, manifestaciones o disturbios?	0
Hay personalidades como fanáticos dentro nuestros clientes del negocio?	0
FUEGO	
El edificio es inflamable dentro de edificio?	0
Las personas tienen interior de seguridad, si edificio? Normas de seguridad está llevado?	0
Si no, ¿podría haber un fuego en su negocio dentro del edificio o donde la gente puede resultar en un caso de emergencia?	0
Ha ha identificado en el alto riesgo de incendio, a raíz de ISO hasta la ocurrencia?	0
Si tiene un, ¿sabe si tienen de extinción?¿Sabe que es posible utilizar en caso de que el punto tomar de acceso este incendiado?	0
El área de cada número tiene una calidad la cual que propia cuenta problemática o calma o tampoco que cada tiempo de una explosión?	0

INCLUIDOS	Valoración
¿Alguno o todos sus procesos críticos de negocio dependen de la energía eléctrica? [E], mecánica eléctrica o electrónica?	0
¿Tiene una fuente de energía para el edificio?	0
Hay algún entendimiento de cómo la de energía eléctrica o otros problemas que podrían afectar a cualquier equipo eléctrico sensible? [E], computadoras)	0
¿Existe un mantenimiento de la energía y sistema de prima?	0
Hay una UPS instalada para garantizar la continuidad del negocio?	0
¿Hay un generador de respaldo disponible? [Generadores eléctricos]	0
¿Cuánto depende de su negocio en la energía eléctrica?	0
¿Tiene pruebas regularmente?	0
¿Tiene su proveedor contactos?	0
Son plantas eléctricas están en un lugar seguro o es posible que alguien no autorizado los manipule?	0
AGUA	
¿Alguno o todos sus procesos críticos de negocio dependen de las conexiones de gas? [G, humo]	0
¿Las conexiones están adecuadamente protegidas?	0
Contaminación del Agua	
¿Alguno o todos sus procesos críticos de negocio dependen de las conexiones de agua? [S], refrigeración o procesos de trabajo	0
¿Las conexiones están adecuadamente protegidas?	0
Mal funcionamiento del equipo	
¿Alguno o todos sus procesos críticos de negocio dependen de ciertos individuos por su conocimiento técnico o habilidad?	0
Se encuentran definidas y documentadas todas la funciones y responsabilidades?	0

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

COMUNICACIONES	Valoración
Red y Telefonía	
¿Su negocio depende de las comunicaciones?	0
¿Hay redundancia en las principales líneas de comunicación?	0
¿Tiene contingencia alternativa?	0
¿Cómo sabría si algo falla en su red/línea o alrededor?	0
¿Existe algún servicio de telecomunicaciones esencial? En caso, que funciones estarían paradas si no tuviera esa capacidad/servicio/red	0
En caso afirmativo, ¿Tiene una contingencia?	0
Infraestructura	
¿Alguna o todas sus funciones de negocio críticas dependen de una ubicación física local (Edificio)?	0
¿Hay un punto único para fallar, tales ubicaciones de conexión dentro del edificio/recinto?	0
¿Cuál es el impacto si no hay acceso a la ubicación durante 1 día?	0
¿Alguna o todas sus funciones de negocio críticas dependen de una Red de área Amplia (WAN)?	0
¿Las líneas están protegidas de interferencias?	0
¿Tiene cortes de redundancia de conectividad?	0
En resumen, ¿intervención mínima/ pasos necesarios para restituir los cuentas?	0

PROTECCIÓN DE DATOS	Valoración
¿Existe una política de seguridad para la información?	0
¿Alguna Ley está vinculada (como Protección de Datos) que afecte a los negocios?	0
Cabe, los registros, que podemos considerar información crítica se mantienen en una habitación privada y segura?	0
Cabe, los registros, se mantienen bajo llave?	0
Cabe, los registros, se encuentran almacenados usando los cuotas de llaves?	0
¿Cualquier personal no autorizado puede tener acceso a esos registros?	0
¿Existe un procedimiento clasificación de registros para acuerdos con diferentes niveles como el Bosa, Importante, Alto, con CONFIDENCIAL?	0
¿Los registros clasificados están almacenados para indicar su nivel de seguridad?	0
¿Los medios de seguridad en el lugar como libre en la clasificación de registros?	0
Seguridad	
¿El personal es propietario de cualquier dispositivo de autor adquirido bajo licencia, ¿Que está adaptado.	0
¿Existe una política de uso de software inaceptable?	0
¿Alguien tiene el poder de instalación permitido en pasar también si hay software no autorizado?	0
¿Hay redundancia de esas auditorías?	0
¿Existe un acceso regular a esa cinta?	0
Recursos Humanos	
¿Existe un proceso de selección para empleados y todos?	0
¿Son esenciales las claves para actividades bajo riesgo de personal/contratos?	0
¿Los contratos son verificados con frecuencia?	0
¿Al finalizarse todos los vacunas de los negocios cuando se evita en uso?	0
¿Existe los algoritmos de cifrado/encriptación SHA-2? Es para encriptar y controlados de forma adecuada?	0
¿El usuario la configuración para información sensible de la vulnerable?	0
La información sensibles es transmitidas por canales dedicados y aplicando altos estándares de seguridad?	0
¿Los comportamientos personales existe? Es mismo asegurados contra robo?	0
¿La organización tiene un seguro contra el robo de equipos ?	0
¿Se informa sobre la seguridad del sitio web de los empleados?	0

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

PLANES DE CONTINGENCIA	Valoración
Prevención	
¿Tienen una alterna que podría ser utilizada para albergar todas las funciones críticas del negocio?	1
¿Si una alterna tiempo a la funcionalidad?	1
¿Si una alterna tiempo en la posibilidad cuando?	1
¿Si una tiene energía eléctrica?	1
¿Si una tiene para email de salida?	1
¿Si una tiene aseo?	1
¿Si una tiene conexiones de comunicación y red?	1
¿Tienen planes del área?	1
Recuperación	
¿Tiene identificados los procesos de negocios críticos?	1
¿Hay planes de recuperación para todos los servicios y procesos críticos de la empresa?	1
¿Son planes actualizados en los últimos seis meses?	1
¿Existe un plan de continuidad de negocio que abarca toda la empresa?	1
¿El plan se ha probado en los últimos seis meses?	1
¿Existe un plan de emergencia?	1
¿El plan se ha probado en los últimos seis meses?	1
¿Existe un plan de recuperación de desastres informáticos?	1
¿El plan se ha probado en los últimos seis meses?	1
Control de cambios	
¿Se limitado modifica para tener acceso remoto en caso de emergencias?	1
¿Existe un software especial diseñado para la mantención remota de equipos?	1
¿Los manuales y procedimientos del área están siendo bien mantenidos?	1
¿Existen procedimientos documentados del servicio de todos los sistemas?	1
¿Existe un equipo experto de fuera de la empresa que maneja la operación del centro en todos y puede realizar la operación?	1
¿Los copias de seguridad están protegidas fuera de la compañía?	1
¿Están documentados los procedimientos de como retomar los actividades requeridas después de retomar los Back de Datos?	1
¿Existe un procedimiento formal que detalle todas las posibilidades registradas y alternativas en caso de [illegible]?	1
¿Existe un [illegible] y en caso de [illegible] el de mantenimiento, ¿El dispositivamente encargado del Data Center puede reestablecer los servicios en otro ubicación de [illegible] ?	1
¿Existe un [illegible] de equipos informáticos y de comunicación de que la [illegible] de [illegible] de [illegible] requerimientos de energía, refrigeración, requerimientos de espacio, equipo suministro y una copia de esta Data Center [illegible] fuera de la compañía?	1

DISEÑO DE UN MARCO METODOLÓGICO PARA EL DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO

Clasificación	
Acceso	2
Seguridad	2
Almacenamiento	1
Ventilación	1
Peligros	1
Explosión	2
Recursos	1
Comunicación	2
Protección de datos	2
Planes de Contingencia	2

Para gestionar los riesgos detectados y mitigarlos en la medida de lo posible, s e propone la puesta en marcha de las siguientes acciones o contramedidas:

PLAN DE ACCIÓN	PRIORIDAD
Instalar antivirus en todos los equipos de la compañía	2
Instalar sistemas de detección de incendios junto con sistemas de extinción	2
Establecer estrategia de copia de seguridad y recuperación de datos incluyendo el almacenamiento fuera del sitio	1
Implementar una política de seguridad informática	2
Implementar un herramienta de monitorización de eventos a fallos en los sistemas, servidores, redes, cambios de temperatura, humedad en el centro de datos	2
Establecer un sistema de alimentación ininterrumpida que se utilizará en caso de fallo en	1
hardware, sistemas y redes vitales.	1
Aplicar controles de seguridad física en todo el edificio	2
Realizar revisiones periódicas los perfiles asignados a los usuarios para acceder a las aplicaciones, archivos y bases de datos y detectar en qué casos los permisos asignados no concuerdan con los previamente definidos para cada perfil.	2
Selección y contratación de seguros	2
Implementar prácticas en las que se identifiquen y transfiera el capital intelectual (conocimiento) de la empresa, involucrando a todo el personal	1
Diseñar planes de recuperación para los procesos de negocio críticos	1
Diseñar planes de recuperación para posibles daños informáticos	1

ESTRATEGIA DE RECUPERACIÓN

De las alternativas existentes y dado que la opción de subcontratar espacios y soporte a terceros resultaría muy costosa para AMBUQ E.P.S., la solución más adecuada sería utilizar la sede de Cartagena como alternativa en caso de incidente grave. De esta forma AMBUQ E.P.S. podría seguir dando servicio a sus clientes, sin que el impacto tuviera consecuencias catastróficas para la compañía. Para ello, podrán utilizarse en primera instancia los equipos que se utilizan en est a sede, de forma que se reaproveche la inversión. Para que estos equipos sean válidos será necesario equipar la infraestructura con algunos elementos extras (servidores, comunicaciones, incremento de memoria, capacidad de disco, etc.).

DESARROLLO E IMPLEMENTACION DEL PLAN

Una vez que se ha seleccionado la estrategia de continuidad, se puede comenzar a construir el Plan de Continuidad definiendo la estructura y composición de los equipos y las acciones de cada uno de ellos. Teniendo en cuenta que AMBUQ E.P.S., es una empresa de tamaño medio, reduciremos el número de equipos y su composición, que serán necesarios en caso de activación del Plan de Continuidad.

Definir y organizar los equipos

Comité de Crisis

ROL	NOMBRE	TELEFONO	TELEFONO DE LA CASA
Director del comité de Crisis	Julieta Daza	3362200	3757621
Miembros del Comité	Gustavo Acosta	3757621	3757621
	Arturo Dorantin	3757621	3757621
	Jorge Salcedo	3757621	3757621

Una vez que se comunica un incidente, el Comité de Crisis debe reunirse y tomar decisiones para afrontar la situación. Deben estar continuamente informados de la situación y determinar si es necesario iniciar el Plan de Continuidad. En este caso, se comunicará a los responsables de los equipos del comienzo de las actividades que llevarán a restablecer los servicios en la sede de Cartagena.

Equipo de Recuperación

ROL	NOMBRE	TELEFONO	TELEFONO DE LA CASA
Administrador de Instalaciones de Recuperación	GustavoGarcía	3362200	3717621
Miembros del Equipo	John Vega	3757621	3717621
	Oscar Robles	3757621	3717621
	Freddy Padilla	3757621	3717621

El equipo de recuperación es el encargado de poner en marcha todo el proceso de recuperación para restaurar los servicios en la sede de Cartagena. Para ello realizarán las siguientes actividades:

- Se trasladarán por transporte terrestre hasta el sitio alterno.
- Pondrán en marcha los sistemas por orden de criticidad y utilizando las copias de seguridad que periódicamente se envían al sitio alterno.
- Inicialmente se reutilizarán los equipos ubicados en la sede alterna para iniciar los servicios. Se contactará con la persona responsable de logística para que solicite a los proveedores todos los equipos y material necesario (servidores, PC's, impresoras, etc.) en los plazos acordados.
- Una vez que se vayan restaurando los servicios, deben comprobar su operatividad.

Equipo de Coordinación Logística

ROL	NOMBRE	TELEFONO	TELEFONO DE LA CASA
Miembros del Equipo	Nubia Hernández	3462300	3757621
	Zaida Díaz	3757621	3757621

El equipo de coordinación logística es responsable de todo lo relacionado con las necesidades logísticas. En función del tipo de incidente se encargará de:

- Atender las necesidades logísticas de primera instancia tras la contingencia. (Transporte de personas, transporte de materiales, etc.)
- Contactar con los proveedores para solicitar el material necesario que indiquen los responsables de la recuperación.
- Reservar habitaciones de hotel en Cartagena para las personas que se desplacen a este sitio.
- Gestionar el suministro de comida al personal involucrado.

Agencia	Nombre de Contacto & Compañía	Teléfono
Hardware	RADIAN Contacto: Jaime Duque	3757621
	DELL Contacto: Mauricio Correa	3757621
Software	Stark Pointer Contacto: Rosa Chinos	3757621
Redes y Comunicaciones	Alcatraz Contacto: Jorge Mercado	3757621
Material de Oficina	Tactos Office Contacto: Jorge Bedoya	3757621
Almacenamiento fuera de sitio	Tostrans Ingeniería Contacto: Oscar Toledo	3757621
Prensa	El Heraldo Contacto: Luis Beltrán	3757621
Servicios Públicos	Electricaribe	116
	ERA	116
Servicios de Transporte	Berlinas	3757621

Equipo de Relaciones Públicas

ROL	NOMBRE	TELEFONO	TELEFONO DE LA CASA
Miembros del Equipo	Juan Manuel Pérez	3362400	3757621
	Ana María Medina	3757621	3757621

El equipo de Relaciones Públicas es responsable de comunicar las decisiones y situación de la empresa durante la contingencia. Las tareas a realizar serán

- Si el tipo de incidente lo requiere, emitir un comunicado oficial a clientes y proveedores en el que se indique que se restablecerán los servicios lo antes posible.
- Atender a los clientes para proporcionarles información sobre el incidente y tranquilizarlos lo máximo posible.

Equipo de las unidades de negocio

Unidad de Negocio	Responsable	Teléfono
Recursos Humanos	Camilo Valdivieso	3757621
Aseguramiento	Oneida Torres	3757621
Financiero - Contabilidad	Nelly Caballero	3757621
Atención al Cliente	Carlos Ordoñez	3757621

Estos equipos estarán formados por las personas que trabajan con las aplicaciones críticas, y serán los encargados de realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas.

Desarrollar los procedimientos

PROCEDIMIENTOS DE RECUPERACIÓN

Procedimiento de notificación del desastre

Cualquier empleado de AMBUQ E.P.S. que sea consciente de un incidente grave que pueda afectar a la empresa, debe comunicarlo al Jefe de Seguridad de la Planta proporcionando el mayor detalle posible en la descripción de los hechos.
El Jefe de Seguridad debe evaluar la situación e informar al Director del Comité de Crisis.

Procedimiento de Lanzamiento del Plan

El Comité de Crisis reunido en el punto de encuentro evaluará la situación. Con toda la información de detalle sobre el incidente, se decidirá si se activa o no el Plan de Continuidad de Negocio. En caso afirmativo, se iniciará el procedimiento de ejecución del Plan. En el caso de que el Comité decidida no activar el Plan de Continuidad porque la gravedad del incidente no lo requiere, si será necesario gestionar el incidente para que no aumente su gravedad.

Los siguientes criterios de decisión se derivan de los umbrales de tolerancia de negocios, obtenidos del análisis de impacto de la compañía.
Un desastre se debe declarar cuando es probable (es decir, más del 50% de probabilidad) que la operación de una unidad o función de negocio de la compañía, estará interrumpida por 48 horas o más.
Un desastre se debe declarar cuando es probable (es decir, más del 50% de probabilidad) que más del 50% de la operación de una ubicación (sede) de la empresa, estará interrumpida por 24 horas o más.
Los equipos de recuperación se debe poner en modo de espera cuando es probable (es decir, más del 50% de probabilidad) que cualquiera de las condiciones anteriores se confirmará en las próximas 12 horas.

Procedimiento de notificación de la puesta en marcha del Plan a los equipos implicados

Activar el árbol de llamadas para avisar a los integrantes de los diferentes equipos que van a participar en el Plan.

Procedimiento de concentración y traslado de equipos

Una vez avisados los equipos y puesto en marcha el Plan, deberán acudir al centro de reunión indicado. Además del traslado de personas a la sede en Cartagena hay que trasladar todo el material necesario para poner en marcha el centro de recuperación (cintas de respaldo, material de oficina, documentación). Esta labor queda en manos del equipo logístico.

Procedimiento de puesta en marcha del centro de recuperación

Una vez que el equipo de recuperación llegue al sitio de alterno ubicado en Cartagena y que los materiales empiecen a llegar, pueden comenzar a instalar las aplicaciones en los equipos que se encuentran en esta oficina. El equipo de recuperación solicitará al equipo de logística cualquier tipo de material extra que fuera necesario para la recuperación.

Procedimientos de restauración

El orden de recuperación de las funciones se realizará según la criticidad los sistemas y RTO establecidos.

Nota En este apartado deberá indicarse el procedimiento concreto de recuperación de cada uno de los sistemas.

Procedimiento de soporte y gestión

Una vez recuperados los sistemas, se avisará a los equipos de los departamentos que gestionan los sistemas (listado del equipo de Unidades de Negocio) para que realicen las pruebas necesarias que certifiquen que funcionen de manera correcta y pueda continuarse dando el servicio. Además el Equipo de Seguridad deberá comprobar que existen las garantías de seguridad necesarias (confidencialidad, integridad, disponibilidad) antes de dar por terminada la fase de recuperación.

FASE DE VUELTA A LA NORMALIDAD

Una vez con los procesos críticos en marcha y solventada la contingencia, hay que plantearse las diferentes estrategias y acciones para recuperar la normalidad total de funcionamiento. Se deberá realizar una valoración detallada de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad. Para ello, el equipo de recuperación junto con el equipo de seguridad, realizarán un listado de los elementos que han sido dañados gravemente y son irrecuperables, así como de todo el material que se puede volver a utilizar. Esta evaluación deberá ser comunicada lo antes posible al equipo director para que determinen las acciones necesarias que lleven a la operación habitual lo antes posible.

El Comité de Crisis contactará con el seguro de la compañía para conocer qué parte cubre el seguro (dependiendo del tipo de póliza contratada por AMBUQ E.P.S.) y qué inversión tendrá que hacer la compañía en el material que no se

puedá recuperar. Contactar con los proveedores para que en el menor tiempo posible reponga todos los elementos dañados.

Dependiendo de la gravedad del incidente, la vuelta a la normalidad de operación puede variar entre unos días (si no hay elementos clave afectados) e incluso meses (si hay elementos clave afectados). Lo importante es que durante el transcurso de este tiempo de vuelta a la normalidad, se siga dando servicio a los clientes y trabajadores por parte de la compañía y que la incidencia afecte lo menos posible al negocio.

9. REFERENCIAS BIBLIOGRAFICAS

[1] Emergency Management Forum, 2001. Documentación en línea: http://www.oalridge.doe.gov/external/Home/PublicActivities/EmergencyManagementForum/default.htm?ref.asp.

[2] GASPAR J., 2004. Planes De Contingencia. La Continuidad Del Negocio En Las Organizaciones.

[3] BS – 25999, Sep – 2010. British Standard – 25999. Documentación en línea: http://www.bs25999.com/

[4] ITIL, Sep – 2010. Information Technology Infraestructure Library. Documentación en línea: http://www.itil-officialsite.com/home/home.asp

[5] ISACA, Sep – 2010. COBIT. Control Objectives for Information and related Technology. Documentación en línea: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx.

[6] Bon J., Ene – 2008. Fundamentos de la Gestión de Servicios de TI basada en ITIL V3. Van Haren Publishing, Tercera Edición. Cap 2, pág. 10.

[7] BCI – 2007. Business Continuity Institute Manual de Buenas Prácticas. Traducido por ISMS Forum Spain. Pág. 12 – 15.

[8] BS – 25999-1, 2006. Bussines Continuity Managemente, Part 1. Code of Practice. Pág. 12 – 67.

[9] SkillSoft Corporation – 2007. Managing Infraestructure using ITIL.

[10] Texto ITIL v3 - 'Service Design', 2007. Publicado por Office of Government Commerce. Pág. 125 – 155.

[11] IT Governance Institute, 2010. COBIT 4.1. Pág. 120 – 123.

Con formato: Inglés (Estados Unidos)
Con formato: Inglés (Estados Unidos)
Con formato: Inglés (Estados Unidos)
Con formato: Inglés (Estados Unidos)
Con formato: Inglés (Estados Unidos)